Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Andraž Sraka

Smernice za varen prehod v zasebni oblak

diplomsko delo
na univerzitetnem študiju

Mentorica: doc. dr. Mojca Ciglarič

Ljubljana 2014

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Tematika naloge:

Računalništvo v oblaku prinaša podjetjem in organizacijam številne koristi glede učinkovitosti informacijske podpore in izrabe virov. Odpira pa tudi novo, še slabo raziskano področje varnosti takšnih sistemov, saj tradicionalni pristopi k omrežni in sistemski varnosti niso dovolj. V diplomski nalogi preučite klasična in nova tveganja, ki jih prinašajo oblačne infrastrukture, nato pa sistematično obdelajte vse vidike prehoda v oblak. Osredotočite se na zasebni oblak kot manj tvegano postavitveno obliko. Za posamezne gradnike infrastrukture navedite sezname ukrepov, ki jih mora izvesti podjetje za celovito obvladovanje tveganj. Pri tem izhajajte iz dobrih praks, priporočil proizvajalcev programske in strojne opreme, strokovnih združenj, standardov in zakonodaje. Smernice nazadnje kritično ovrednotite in ocenite njihovo uporabnost v slovenskem prostoru.

Izjava o avtorstvu diplomskega dela

Spodaj podpisani Andraž Sraka, z vpisno številko **63010136**, sem avtor diplomskega dela z naslovom:

Smernice za varen prehod v zasebni oblak

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom doc. dr. Mojce Ciglarič,
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela,
- soglašam z javno objavo elektronske oblike diplomskega dela na svetovnem spletu preko univerzitetnega spletnega arhiva.

V Ljubljani, dne 24. septembra 2014 Podpis avtorja:

Posvečeno Maji, Neži in Luni.

Kazalo

Povzetek

Računalništvo v oblaku prinaša številne prednosti, ki lahko znatno izboljšajo učinkovitost virov IKT v poslovnih procesih. Po drugi strani pa odpira novo poglavje informacijske varnosti, in sicer, kako in na kakšen način zagotoviti varnost podatkov, ki se shranjujejo in obdelujejo kot del storitev računalništva v oblaku. Diplomsko delo povzema raziskave varnostnih tveganj uporabe računalništva v oblaku, ki jih je opravilo združenje CSA (Cloud Security Alliance), in se osredotoča na izgradnjo zasebnega oblaka kot najvarnejše oblike storitev računalništva v oblaku. Namen diplomskega dela je podati smernice, ki lahko pripomorejo k uspešnemu in predvsem varnemu prehodu v zasebni oblak. V ta namen se je za posamezne gradnike infrastrukture zasebnega oblaka pripravilo sezname ukrepov, ki znatno zmanjšajo ali celo izničijo določena varnostna tveganja na podlagi pregleda dobrih varnostnih praks, priporočil posameznih proizvajalcev programske in strojne opreme za gradnjo storitev računalništva v oblaku, varnostnih standardov in zakonodaje.

Ključne besede: računalništvo v oblaku, zasebni oblak, varnost podatkov, dobre prakse, izboljšanje varnosti.

Abstract

Cloud computing brings forth numerous advantages that have a potential to significantly improve the efficiency of ICT business processes. But it also opens a whole new chapter of information security, since it has to deal with ensuring safety of the data that gets stored and processed as a part of services of cloud computing. This diploma thesis summarizes safety risk research conducted by the CSA (Cloud Security Alliance), and focuses on building a private cloud as the safest form of cloud computing services. The aim of this diploma thesis is to provide guidelines that can contribute to a successful and secure transition into a private cloud. To this end, we prepared a list of measures for individual building blocks of the infrastructure of the private cloud that need to be taken in order to reduce or even nullify certain security risks. We composed this list by examining security best practices, recommendations of individual software and hardware vendor, and security standards and legislation.

Keywords: cloud computing, private cloud, data security, best practices, hardening.

Poglavje 1

Uvod

Oblaki že nekaj let niso zgolj vremenski pojav na nebu, temveč se vanje seli celo računalništvo in storitve, povezane z njim. Dejstvo je, da računalništvo v oblaku ni več v povojih; nasprotno, svojo revolucijo naj bi po mnenju ameriškega publicista Nicolasa Carra začelo že pred leti.

Ko govorimo o računalništvu v oblaku, razmišljamo širše in ne zgolj o tehnologiji, ki poganja hitro rastoča tehnološka podjetja. Gre za združitev že znanih in uveljavljenih informacijskih tehnologij in konceptov, ki postaja realnost sodobnega poslovnega in zasebnega sveta. Računalništvo v oblaku je postalo tako nepogrešljivo, kot so samoumevne mobilne aplikacije in vsakodnevno uporabljene spletne storitve, ne glede na to, ali gre za našo najljubšo spletno igro, socialno omrežje ali poslovno aplikacijo.

Krizne razmere v gospodarstvu so v zadnjih letih povzročile, da podjetja računalništvu v oblaku namenjajo vse več pozornosti. Uporabno je prav za vsakogar, ki želi optimizirati svoje okolje IT. Vprašanja, zakaj in ali sploh bi torej izbrali računalništvo v oblaku, si ni več smiselno postavljati. Računalništvo v oblaku je tukaj, deluje in v svetu IT vse bolj kraljuje. Za uspešno uporabo storitev, ki jih računalništvo v oblaku ponuja, pa je ključen "miselni preskok" uporabnikov (najemnikov) storitev, da si več ne lastijo ne

strojne ne programske opreme, ki poganja storitev.

Zelo pomembno pa je vprašanje, kako vstopiti oziroma prestopiti v oblak, da bosta sprememba in uporaba kar se da varni in da bosta pozitivno doprinesli k doseganju poslovnih ciljev. Temelji za to obstajajo. Računalništvo v oblaku ima mnoge prednosti. Od fleksibilnosti do zniževanja stroškov oziroma plačevanja zgolj porabljenega najema storitev v oblaku, povečanja nadzora virov ipd. Vendar pa računalništvo v oblaku prinaša tudi določena tveganja, o katerih se moramo pravočasno seznaniti, jih oceniti in ustrezno ukrepati, da se ne bi udejanjila.

Cilji diplomskega dela se dotikajo prav slednjega. V prvem delu naloge je cilj pregledati največje nevarnosti, ki ogrožajo računalništvo v oblaku, in sicer se ravnamo po raziskavah, ki jih je objavilo združenje CSA (Cloud Security Alliance). V drugem delu pa je cilj na primeru računalniške infrastrukture oblaka nakazati, kako zmanjšati tveganja te vrste groženj. Ker je domena računalništva v oblaku široka, se bomo v diplomskem delu osredotočili predvsem na infrastrukturo kot storitev v postavitvenem modelu zasebnega oblaka, ki ga vzpostavljamo v lokalnem okolju na lastni strežniški infrastrukturi. Osnovni ukrepi bodo zbrani v obliki smernic tega, na kaj moramo z vidika optimalne varnosti paziti, ko se odločamo za izgradnjo zasebnega oblaka, pri čemer upoštevamo ustrezno evropsko direktivo, slovensko zakonodajo in ostale dobre varnostne prakse, ki jih navadno že vpeljujemo v primeru naše “klasične” infrastrukture IKT.

Interes za te smernice je pokazal tudi slovenski odsek CSA, ki želi na podlagi tega diplomskega dela izdati smernice za slovensko strokovno javnost z namenom dvigniti stopnjo ozaveščenosti o tveganjih, ki jih prinaša računalništvo v oblaku, in ponuditi jasnejšo sliko tega, na kaj je treba paziti in kaj upoštevati, ko se lotimo prehoda v zasebni oblak.

Poglavje 2

Računalništvo v oblaku

2.1 Osnovni pojmi in problemska domena

Računalništvo v oblaku kot nov trend IT zadnjih nekaj let ne predstavlja pretirane razvojne inovacije; predstavlja bolj združitev že znanih in uveljavljenih konceptov IT ter manjši "miselni preskok" pri njihovi uporabi. Skupek tehnologij, med katerimi so virtualizacija fizične strojne opreme, virtualizacija omrežij, avtomatizacija in orkestracija, spletne tehnologije (WEB 2.0, spletne storitve s storitveno usmerjeno arhitekturo in spletnimi programskimi vmesniki), tako močno prispeva k uveljavitvi modela, imenovanega računalništvo v oblaku.

Računalništvo v oblaku zagotavlja računalniške vire in funkcionalnosti, ki so na voljo končnim "stanovalcem" in pri tem zanemari podrobnosti tega, kje in kako se to izvaja. S pojmom stanovalec (angl. tenant) bomo označevali uporabnika oziroma najemnika storitve računalništva v oblaku. Stanovalcem so tako zagotovljeni viri vidni kot storitev, ki je v osnovi dostopna prek omrežne povezave.

2.1.1 Virtualizacija kot sestavni del računalništva v oblaku

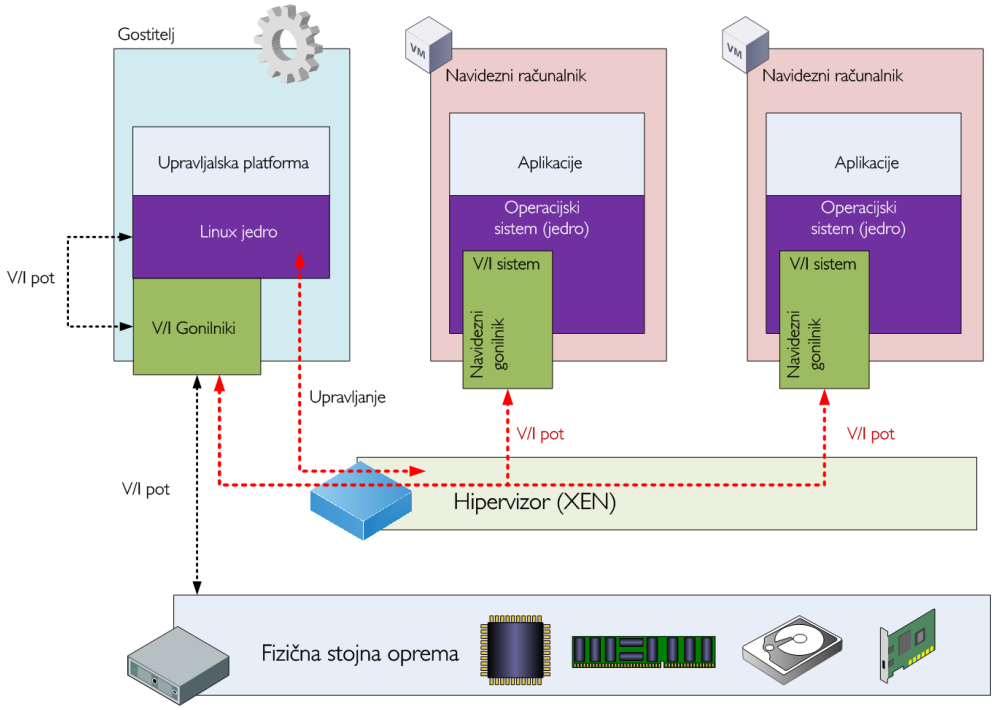
Med zgoraj naštetimi tehnologijami je vredno posebej omeniti predvsem virtualizacijo strojne opreme, ki se vse prevečkrat enači kar s samim pojmom računalništva v oblaku.

Virtualizacija strojne opreme je zgolj ena izmed tehnologij, ki močno zaznamujejo model računalništva v oblaku, ni pa nujno potrebna. Poznamo nekaj implementacij tovrstne "oblačne" infrastrukture in storitev, ki ne temeljijo na virtualizaciji oziroma je sploh ne uporabljajo. Virtualizacija strojne opreme kot tehnologija ni nova in je v poslovnem svetu zelo razširjena, predvsem ko govorimo o učinkovitostih fizičnih strežnikov in izkoriščenosti le-teh. Koncept virtualizacije je abstrakcija fizičnih komponent v logične objekte, kot so na primer strežniki, omrežne naprave, naprave za shrambo ipd. Na ta način skrivamo fizične lastnosti naprav in hkrati omogočamo večjo fleksibilnost in lažje upravljanje z logičnimi objekti.

Obstaja več vrst oziroma ravni strežniške virtualizacije; njena najbolj uporabna in razširjena oblika je polna strojna virtualizacija. Pri temu tipu virtualizacije se privilegirani ukazi gostujočih operacijskih sistemov samodejno izvajajo v hipervizorju (angl. hypervisor). Preverjanje teh ukazov pa je izvedeno neposredno v strojni opremi centralne procesne enote, zaradi česar je tudi hitrost izvajanja večja.

Da lahko omogočimo polno strojno virtualizacijo fizičnega strežnika, potrebujemo na procesorjih strežnikov družine x86 ustrezno podporo strojni virtualizaciji (AMD-v podporo virtualizaciji na procesorjih družine AMD, procesorji družine Intel pa podporo VT-x). Druga komponenta, ki je potrebna, pa je tako imenovani hipervizor, ki doda nivo abstrakcije nad fizično strojno opremo. Hipervizor tudi upravlja z navideznimi računalniki (angl. virtual machine) in skrbi za komunikacijo navideznih računalnikov s fizičnimi komponentami strežnika. Trenutno najbolj razširjeni hipervizorji so: Hyper-V

(Microsoft), ESX/ESXi (VMware), XenServer (Citrix), Xen in QEMU/KVM (odprtokodni).



Slika 2.1: Visokonivojska arhitektura hipervizorja XEN

Virtualizacija strežnikov prinaša večjo izkoriščenost fizične platforme, saj se lahko na enem fizičnem strežniku izvaja več navideznih računalnikov hkrati. Če strnemo, so ključne prednosti virtualizacije:

- možnost sočasnega izvajanja več različnih operacijskih sistemov na enem fizičnem strežniku,
- izoliranost navideznih računalnikov, pri čemer napaka znotraj enega navideznega računalnika ne vpliva na delovanje ostalih. V nadaljevanju bodo predstavljena tudi potencialna tveganja tega, da je mogoče izstopiti iz izoliranega prostora navideznega računalnika,
- celotno stanje navideznega računalnika (delovni pomnilnik, stanje procesorja, stanje operacijskega sistema in aplikacij) je mogoče zaustaviti,

shraniti oziroma celo premakniti na drugo fizično platformo in zagnati ter nemoteno nadaljevati z delom,

- premikanje in kopiranje navideznega računalnika tako postane trivialno. Določeni hipervizorji omogočajo tudi premikanje navideznega računalnika znotraj gruče fizičnih strežnikov v "realnem času"(brez vidnejših prekinitev v delovanju),

- možnost spreminjanja konfiguracije navideznega računalnika (npr. povečevanje delovnega spomina, dodatno število CPE *(centralnih procesnih enot)* ipd.)) med samim delovanjem; odvisno od hipervizorja in operacijskega sistema navideznega računalnika, vendar za vse manjše spremembe vsekakor ni potreben ponoven zagon navideznega računalnika.

Virtualizacija kot tehnologija prinaša mehanizme, ki lahko znatno izboljšajo učinkovitost samih podatkovnih centrov in lahko pripomore pri [1]:

- prihrankih energije (in posredno hlajenju) podatkovnih centrov,
- zmanjšanju fizičnih prostorov za fizične strežnike in opremo,
- boljšemu, predvsem pa hitrejšemu oskrbovanju s strežniki,
- boljši izolaciji med aplikacijami in sistemi,
- nezdružljivosti programske in strojne opreme,
- zmanjšanju stroškov za samo obratovanje.

Vse navedeno navadno prinaša pozitivne učinke na delovanje poslovne organizacije in njene konkurenčnosti na trgu.

2.1.2 Računalništvo v oblaku

Ko poskušamo opredeliti pojem računalništvo v oblaku, naletimo na več različnih definicij:

- NIST *(National Institute of Standards and Technology)* [2] ga opredeljuje kot: "Model za omogočanje omrežnega dostopa do deljenih računalniških virov (omrežje, strežniki, shramba, aplikacije in storitve), ki so lahko hitro oskrbovani in izdani ob minimalnem trudu vodstva oziroma interakciji s ponudnikom storitve."

- UC Barkley [3] pojem pojasnjuje takole: "Gre za aplikacije, strojno opremo in sistemsko programsko opremo znotraj podatkovnih centrov, ki so dostavljene kot storitev preko medmrežja."

Značilnosti oblaka in oblačnih storitev lahko strnemo v naslednje [2]:

- **samopostrežba na zahtevo** (angl. on-demand self-service): končni stanovalec ima možnost oskrbovanja z računalniškimi viri brez potrebe po udeležbi osebja ponudnika. Tovrstna storitev je navadno omogočena z uporabniškim samopostrežnim portalom oziroma spletnim programskim vmesnikom,

- **univerzalen mrežni dostop** (angl. broad network access): vsi računalniški viri in storitve so končnemu stanovalcu na voljo preko omrežja in dostopni preko standardnih mrežnih mehanizmov in protokolov,

- **združevanje virov in večstanovanjski model** (angl. resource pooling and multi-tenancy): vsi računalniški viri oblaka in funkcionalnosti (pomnilnik, procesor, hramba podatkov, aplikacije, ...) so zbrani v bazi virov kot homogena celota in v večini primerov deljeni med različne končne stanovalce oblaka. Deljenje virov omogoča bolj učinkovito izkoriščenost virov. V infrastrukturi javnega oblaka sobiva več stanovalcev, zato je treba zagotoviti ustrezno izolacijo med posameznimi končnimi stanovalci in storitvami, ki jih najemajo/uporabljajo,

- **elastičnost** (angl. elasticity): elastičnost je ena izmed najbolj pomembnih značilnosti računalništva v oblaku. Ta lastnost omogoča, da lahko dinamično dodajamo in odstranjujemo kapacitete virov v skladu s trenutnimi potrebami. Razpoložljivi viri so stanovalcu na voljo v takojšen zakup. Elastičnost končnemu stanovalcu prinaša možnost bolj prilagodljivega načrtovanja kapacitet in posredno vpliva na stroške izvajanja storitve,

- **merjenje storitev** (angl. measured service): poraba vseh oblačnih virov je merjena v času in zmogljivosti, kar predstavlja osnovo, na podlagi katere se končnemu stanovalcu lahko zaračuna dejanska uporaba storitve. Sam ponudnik/upravljavec oblaka pa ima natančen pregled porabe vseh virov v oblaku.

2.1.3 Postavitveni modeli računalništva v oblaku

Računalništvo v oblaku delimo na več postavitvenih modelov glede na to, komu so namenjene storitve in viri računalništva v oblaku ter kje se infrastruktura oblaka nahaja. Tako v grobem poznamo javni oblak, zasebni oblak, skupnostni oblak ter hibridni oblak, ki povezuje storitve zasebnega oblaka s storitvami javnega oblaka.

Javni oblak

Najpopularnejša oblika postavitvenega modela računalništva v oblaku je tako imenovani javni oblak (angl. public cloud), pri katerem so infrastruktura oblaka in viri deljeni med več stanovalcev. Infrastruktura je navadno v upravljanju in lasti ponudnika računalništva v oblaku. Storitve so dosegljive preko interneta in s strani ponudnika zaračunane glede na dejansko porabo. Uporaba storitev javnih oblakov prinaša celo vrsto tveganj in groženj, ki izvirajo ravno iz dostopnosti od vsepovsod ter delitve računalniških virov med več stanovalcev, ki so lahko tudi zlonamerni. Več o posameznih tveganjih, ki

postavljajo uporabo računalništva v oblaku pod vprašaj, opisujemo v naslednjem poglavju. Bolj znane rešitve javnega oblaka so Amazon Web services, Microsoft Azure, Google Cloud in Google AppEngine.

Zasebni oblak

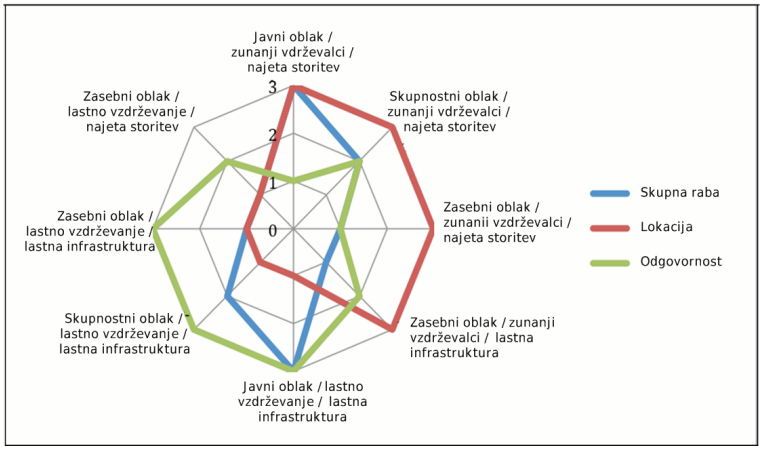
Zasebni *(privatni)* oblak (angl. private cloud) je računalniška infrastruktura in ostale storitve računalništva v oblaku, ki so dostopne samo v zasebnem omrežju. Storitve informacijsko-komunikacijske tehnologije (IKT) so ponujene iz lastnega podatkovnega centra ali najete pri ponudniku tovrstnih storitev. Fizična infrastruktura je navadno ločena oziroma uporabljena zgolj in samo za naročnika, ki tovrstni zasebni oblak najema. Vse storitve in tudi infrastruktura so pod nadzorom ponudnika, upravljanje pa se lahko izvaja tudi s pomočjo tretjega subjekta. Storitve so dostopne preko interneta ali preko navideznih zasebnih omrežij (angl. Virtual Private Network – VPN). Se pa implementacija zasebnega oblaka od ponudnika do ponudnika razlikuje, kot se razlikuje tudi dogovorjena raven storitev (angl. Service Level Agreement – v nadaljevanju SLA), ki jo ponudnik zagotavlja v okviru nudenja zasebne infrastrukture v oblaku.

Skupnostni oblak

Pojavlja se tudi oblika skupnostni oblak (angl. community cloud), ki še najbolj spominja na javni oblak, z glavno razliko, da ima omejeno število stanovalcev z znanimi (skupnimi) značilnostmi. Primeren je predvsem za akademske mreže in ostale zaprte kroge uporabnikov, kot so npr. poslovni inkubatorji. V Sloveniji tak tip storitev v oblaku ponuja organizacija ARNES članom akademsko-raziskovalnega omrežja.

Hibridni oblak

Hibridni tip oblaka (angl. hybrid cloud) so storitve računalništva v oblaku, ki jih sestavljajo storitve javnega in zasebnega oblaka. V porastu je tovrstna hibridna rešitev in možnost razširitve (angl. cloud-bursting)[3] zasebnega oblaka, ko se povečajo potrebe po dodatnih virih, ki jih znotraj zasebnega oblaka ne moremo zagotoviti za nemoteno izvajanje storitev. Danes vse več programske opreme za orkestracijo in upravljanje posameznih komponent zasebnega oblaka omogoča enostavno širitev tovrstnih storitev v enega od javnih oblakov.



Slika 2.2: Primerjava postavitvenih modelov v povezavi s skupno rabo, lokacijo in odgovornostjo

2.1.4 Tipi storitvenih modelov in razmejitev odgovornosti

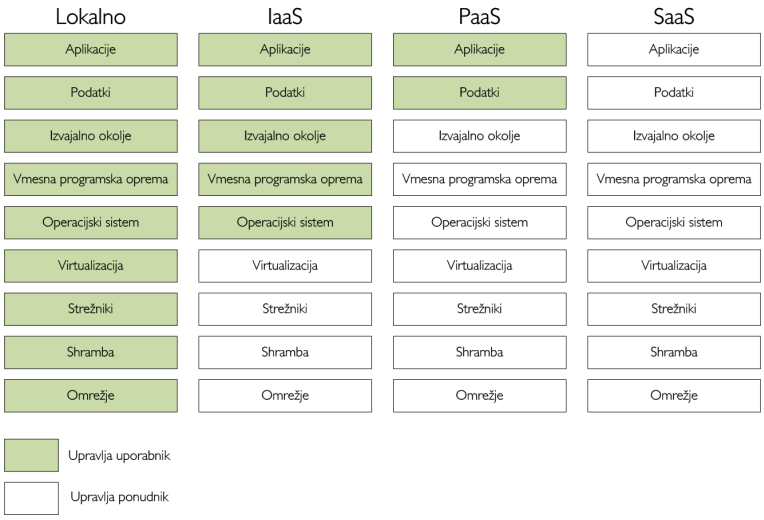
Storitveni model oblaka predstavlja večslojno abstrakcijo osnovnih razredov storitev, ki jih zagotavlja model računalništva v oblaku in definira ustrezno povezavo med posameznimi nivoji. Publikacija NIST [2] definira tri osnovne storitvene modele oblaka, in sicer *infrastrukturo kot storitev – IaaS*, *platformo*

kot storitev – PaaS in *programsko opremo kot storitev – SaaS*.

Infrastruktura kot storitev (angl. Infrastructure as a Service – IaaS) Zajema upravljanje na nivoju računalniške infrastrukture oblaka in daje stanovalcu največjo fleksibilnost, da si zgradi in vzpostavi dotično infrastrukturo glede na potrebe in želje, ter na stanovalca preloži odgovornost postavitve in vzdrževanja vsega od operacijskega sistema dalje.

Platforma kot storitev (angl. Platform as a Service – PaaS)
Običajno že vključuje dodatne funkcionalnosti v obliki programskega vmesnika, preko katerega stanovalec uporablja platformo pri razvoju in upravljanju lastne rešitve IKT, ki teče na najeti platformi. Stanovalec ima bistveno manjšo fleksibilnost in mora delovanje svoje aplikacije navadno zelo prilagoditi ustreznim omejitvam platforme; ponudnik pa prevzame vso odgovornost za delovanje vseh nižjih komponent, ki poganjajo platformo. Vidnejši ponudniki platform kot storitev so: Amazon Elastic Beanstalk, Google AppEngine, RedHat Openshift, Heroku, Windows Azure Websites.

Programska oprema kot storitev (angl. Software as a Service – SaaS) Ponudnik zagotavlja celotno infrastrukturo skupaj s programsko opremo in nastavitvami za njeno delovanje. Vidnejša programska oprema, ki jo je moč najeti kot storitev, je: Microsoft Office 365, Google Apps, Salesforce CRM itd.



Slika 2.3: Tipi storitvenih modelov računalništva v oblaku

Posamezni nivoji predstavljajo tudi razmejitev odgovornosti med stanovalcem in ponudnikom. Ta je odvisna od tega, kakšno storitev naročnik uporablja oziroma v kolikšnem obsegu upravljavec platforme *(navadno ponudnik)* nudi upravljano storitev, običajno v obliki dogovorjene ravni storitve (SLA). Računalništvo v oblaku je tako fleksibilno, da lahko najemamo samo določen tip storitve oziroma funkcionalnosti. Upravljanje in skrb za delovanje in varnost vseh vmesnih elementov, ki so potrebni, da ta storitev deluje, lahko tako prepustimo ponudniku računalništva v oblaku oziroma storitve.

2.2 Prednosti in slabosti rešitev računalništva v oblaku

Iz zgornjega opisa, zlasti pa iz obstoječe prakse lahko razberemo, da računalništvo v oblaku prinaša mnogo tehničnih, pa tudi finančnih prednosti za organizacijo oziroma končnega stanovalca. Lastnosti, ki lahko poslovni organizaciji ali posamezniku prinesejo vrsto prednosti, so:

- **povečanje nadzora virov IT:** če organizacija ni imela pregleda nad lastno porabo virov IT/računalniških virov, bo z najemom oblačnih sto-

ritev pridobila tovrsten pregled, ker bo ponudnik oblačnih storitev skrbel za nadzor in beleženje porabe, ki je nujen že zaradi zaračunavanja porabljenih virov,

- **najem računalniških virov na zahtevo:** take vrste najem se lahko izkaže za eno največjih prednosti oblačnih storitev, saj se organizacija tako izogne začetni investiciji nakupa lastne strojne opreme in vzpostavitve. Hkrati pa ima vso fleksibilnost, da glede na trenutne potrebe najema računalniške vire in ostale funkcionalnosti. To navadno še posebej razveseljuje razvijalce aplikacij, ker postanejo tako bolj fleksibilni. Ker se zmanjšajo zamude s pripravo in konfiguracijo razvojnega, testnega in izvajalnega okolja, se pospeši razvoj. Poslovne organizacije se lahko v celoti posvečajo primarnim ciljem in smotru poslovnega procesa,

- **skoraj "neomejena"(s)hramba za podatke:** oblačne storitve so tako raztegljive, da je možno kapaciteto računalniških virov prilagajati željam in potrebam stanovalca,

- **enostavna načrtovanja obnovitev po katastrofi:** med storitvami računalništva v oblaku se pojavlja tudi izvajanje varnostnega kopiranja podatkov ali celo kopiranja infrastrukture oziroma navideznih računalnikov na zahtevo. To lahko znatno pohitri in izboljša načrtovanja in obnovitev po katastrofah, če le pravilno uporabimo tovrstne storitve računalništva v oblaku.

Po drugi strani pa imajo storitve v oblaku tudi svoje pomanjkljivosti. "Deževna"(slaba) stran storitev računalništva v oblaku v poslovnih organizacijah vzbuja nezaupanje in preprečuje, da bi se organizacije hitreje odločale za njihovo uporabo oziroma selitev v oblak v celoti. Izpostavimo samo najbolj kritične:

- **morebitni tehnični problemi**, ki lahko nastopijo pri prehodu v oblak. Izkaže se namreč, da za vsako "oblačno storitev", za vsakega ponudnika računalništva v oblaku veljajo določene tehnične in funkcionalne

zahteve in omejitve, ki jih mora končni stanovalec upoštevati tako pri prehodu v oblak kot tudi pri načrtovanju aplikacije, ki se bo izvajala v oblaku. Ponudniki računalništva v oblaku navadno nudijo določeno raven in funkcionalnost svojih storitev, ki jih stanovalec ob prijavi (uporabi) storitve sprejme, a naleti na težave, ko te omejitve doseže iz razloga "napačne" uporabe ali višje sile oziroma samega delovanja oblaka. Poglejmo konkreten primer: ponudnik Amazon za določen tip storitve hrambe podatkov S3 (Amazon Simple Storage Service) zagotavlja, da podatkov v oblaku ne bomo nikoli izgubili, vendar hkrati ne zagotavlja, da bodo ti podatki vedno v celoti (v vsakem trenutku) na voljo oziroma dosegljivi preko medmrežja. V nadaljevanju se prav tako pojavi vprašanje, kako stopiti v oziroma izstopiti iz oblaka ali zamenjati ponudnika in pri tem upoštevati omejitve starega in novega ponudnika ter to ustrezno načrtovati pri samem prehodu,

- **problem razlikovanja med odgovornostmi stanovalca in ponudnika storitve v oblaku**, ki se posredno kaže skozi opisane potencialne tehnične težave, na katere naleti končni stanovalec. Najemnik se mora zavedati, kaj mu ponudnik glede na vrsto oblaka in vrsto storitve, ki jo najema, zagotavlja in za kaj odgovarja. Tovrstna dogovorjena raven storitev (SLA) se za vsako storitev razlikuje, kot se razlikuje tudi med posameznimi ponudniki storitev računalništva v oblaku,

- **zmogljivost aplikacij v oblaku ni nujno boljša**, kar predvsem velja za javne oblake. Ker so računalniški viri deljeni med več najemnikov, lahko to vpliva na odzivnost aplikacij. Vpliv ima tudi latenca omrežja, če upoštevamo, da dostopamo do aplikacije preko medmrežja oziroma interneta. Z upoštevanjem vseh tovrstnih lastnosti, tehničnih omejitev oblaka ter s pametnim načrtovanjem aplikacij za delo v oblaku je mogoče ta problem omiliti,

- **organizacija in zaposleni**: pri računalništvu v oblaku gre za združitev že znanih in uveljavljenih informacijskih tehnologij in konceptov, ključen

pa je "miselni preskok"pri njihovi uporabi. Tako so lahko prav ljudje v organizaciji svojevrstna ovira pri uspešnem prehodu in uporabi storitev v oblaku. Govorimo o prilagajanju na relativno nove koncepte uporabe, ki zahtevajo določeno mero izobraževanja. Vse prevečkrat pa se ljudje v podjetjih bojijo sprememb, so ozkogledi in se osredotočajo na slabosti in pomanjkljivosti, namesto da bi izkoristili prednosti, ki dolgoročno zagotovo olajšajo, pospešijo in pocenijo doseganje poslovnih ciljev. Pri prehodu na računalništvo v oblaku pa je pomembno, da potezo podpira tudi najvišje vodstvo v organizaciji, ne le ekipa IT. Vodstvo je namreč tisto, ki določa vizijo, pripravlja strategijo podjetja in širi vrednote ter organizacijsko kulturo, kateri mora slediti sleherni zaposleni. Če bo vodstvo ocenilo in zaposlenim sporočalo, da je računalništvo v oblaku za podjetje dobra izbira, ter jim razložilo, kaj omogoča, bodo zaposleni spremembo tudi lažje sprejeli,

- **varnost storitev v oblaku** v diplomskem delu posebej obravnavamo v naslednjem poglavju, v katerem so predstavljena glavna varnostna tveganja, povezana s storitvami računalništva v oblaku,

- **problem zaupanja podatkov oblaku**, ki se delno dotika varnosti storitev v oblaku, neposredno pa izpostavlja pomembno vprašanje glede varnosti podatkov, ki s storitvami v oblaku zapuščajo naše interno poslovno omrežje, morda celo državo in s tem prihajajo v nasprotje z lokalnimi zakoni in regulativami o varstvu podatkov.

2.3 Varnost računalništva v oblaku in izzivi

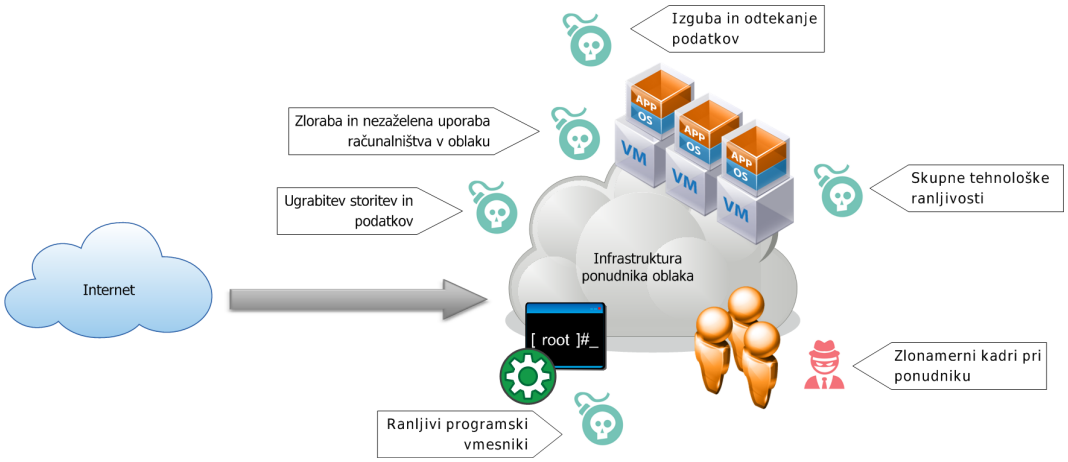
Pri uporabi storitev računalništva v oblaku se je treba zavedati tveganj, ki jih uporaba prinese. Iz opisa v zgornji točki lahko strnemo, da se podatki lahko hranijo in obdelujejo pri zunanjem ponudniku storitev, kar prinaša določene pravne omejitve in zahteve. Upoštevati je treba tudi, da gostovanje na javnih infrastrukturah omogoča vpliv (sumljivih) "sostanovalcev", ki lahko ogrožajo

poslovanje poslovne organizacije, ki najema storitve.

Združenje **Cloud Security Alliance (CSA)** je neprofitna organizacija, namenjena promoviranju uporabe najboljših praks za zagotavljanje varnosti računalništva v oblaku in temu, da nudi izobraževanja s področja uporabe računalništva v oblaku z namenom zaščite vseh ostalih oblik računalništva; pozorno spremlja trende in tveganja, ki jih računalništvo v oblaku prinaša. Združenje je v okviru delovne skupine "CSA Top Threats Working Group" objavilo tudi seznam največjih tveganj pri uporabi računalništva v oblaku, ki jih je objavilo v naslednjih dveh publikacijah na naslovu [4].

- *Top Threats to Cloud Computing* [5] je dokument iz leta 2010, ki izpostavlja in opisuje najbolj kritična varnostna tveganja pri uporabi računalništva v oblaku. Med ključna tveganja, razvrščena od bolj do manj kritičnih, se tako uvrščajo: zloraba in nezaželena uporaba storitev računalništva v oblaku, ranljivi programski vmesniki, zlonamernost osebja ponudnika, ki ima dostop do podatkov v oblaku, skupne tehnološke ranljivosti, izguba in odtekanje podatkov, odtujitev uporabniškega računa in storitev in ostala, neznana tveganja.

- *The Notorious Nine Nine Cloud Computing Top Threats* [6] je posodobljena verzija z na novo razvrščenimi tveganji glede na kritičnost, ki jih zadnja, dopolnjena raziskava delovne skupine CSA prinaša.



Slika 2.4: Najbolj izpostavljena tveganja računalništva v oblaku

Ranljivi programski vmesniki – ena izmed glavnih lastnosti računalništva v oblaku so spletni programski vmesniki, s pomočjo katerih je mogoče na enostaven in fleksibilen način od vsepovsod (predvsem ko govorimo o javnih oblakih) upravljati oblačno infrastrukturo in njene storitve. Programski vmesniki so navadno javno dostopni na internetu preko protokola HTTP, pri čemer se pogosto srečamo s slabo implementacijo varnostnih mehanizmov, predvsem avtentifikacije stanovalcev, in neuporabo protokola SSL/TLS za varno/šifrirano spletno povezavo do spletnega programskega vmesnika. Še najbolj pogoste pa so navadnemu uporabniku spletnega programskega vmesnika skrite funkcionalnosti, ki so del nezanesljive oziroma testne programske kode, ki je zaradi hitrega razvoja postala tudi del javnega produkcijskega spletnega programskega vmesnika in tako ogroža delovanje delovanje oblaka. Ker so spletni programski vmesniki javno izpostavljeni na internetu, je verjetnost zavrnitev storitve pri porazdeljenem napadu (angl. distributed denial-of-service – DDoS) toliko večja in v tem primeru je upravljanje oblačnih storitev na daljavo onemogočeno. CSA tveganje te vrste postavlja na 4. mesto 9 najbolj izpostavljenih tveganj, ki jih računalništvo v oblaku prinaša.

Zloraba in nezaželena uporaba računalništva v oblaku – naročnik storitve javnega oblaka si lahko deli infrastrukturo in ostale računalniške vire z različnimi stanovalci (lahko tudi s sumljivimi ali zlonamernimi sosedi), ki izvajajo napade nanj ali druge in lahko tako zlorabljajo računalniške vire, da so storitve v oblaku motene ali celo nedosegljive. Zavedati se je treba, da je mogoče v javnih oblakih, kjer ni več neposrednega osebnega stika med ponudnikom storitve in kupcem, storitve najeti že z ukradeno bančno kartico. Računalniške vire je mogoče uporabiti za omrežje robotskih računalnikov (angl. botnet), ki jih napadalec lahko uporabi za izvajanje zlonamernih dejanj, kot je na primer zavrnitev storitve pri porazdeljenem napadu (DDoS) na neko storitev znotraj ali izven oblaka. Te vrste tveganj CSA umešča na 7. mesto 9 najbolj izpostavljenih tveganj, ki jih računalništvo v oblaku prinaša.

Ugrabitev storitev in podatkov – ker so storitve javnega oblaka javno dostopne preko interneta, je tako verjetnost dostopa do podatkov s krajo upravljavske identitete v kombinaciji z ranljivimi programskimi vmesniki toliko večja. Poleg možnosti odtujitve občutljivih poslovnih podatkov lahko ugrabitev pomeni posredno tudi zlorabo sosedstva v oblaku in nezaželeno uporabo računalniških virov in storitev v oblaku. Tveganje te vrste CSA umešča v zadnji raziskavi bistveno višje, na 3. mesto 9 najbolj izpostavljenih, v primerjavi raziskavo iz leta 2010, ko je bilo na 6. mestu. Glavni razlog je nedvomno povečano število varnostnih incidentov, povezanih s slabim uvajanjem postopkov istovetenja in dodeljevanja pooblastil na vmesnikih za upravljanje storitev v oblaku pri skoraj vseh večjih ponudnikih storitev v oblaku.

Izguba in odtekanje podatkov predstavljata tveganje, ki je posledica tega, da so računalniški viri storitve deljeni med več stanovalcev, da so dostopni od kjerkoli, poleg tega pa gre še za kombinacijo posameznih specifik oblačnih tehnologij skupaj z ranljivimi spletnimi programskimi vmesniki in človeškim faktorjem pri samem upravljanju storitev računalništva v oblaku.

Ta vrsta tveganja predstavlja visoko stopnjo verjetnosti za podatkovne nesreče in neželene prenose oziroma razkritja tako osebnih kot drugih pomembnih podatkov stanovalcev. CSA tveganje te vrste uvršča na sam vrh lestvice najbolj izpostavljenih groženj računalništva v oblaku, saj to pomeni izgubo stanovalca, kar predstavlja tako poslovno kot finančno izgubo.

Skupne tehnološke ranljivosti – uporaba skupne oblačne tehnologije lahko v primeru njene ranljivosti ogrozi podatke in procese vseh naročnikov, ki si delijo iste računalniške vire. V to kategorijo vključujemo predvsem ranljivosti hipervizorja, ki poganja navidezne računalnike. Ranljivost se lahko izkaže kot slaba izolacija določenih pomnilniških delov/komponent (predpomnilnik centralne procesne enote, grafične procesne enote itd.), ki niso bile zasnovane za tako močno izolacijo večstanovanjskega okolja (angl. multitenant). CSA tveganje ocenjuje kot najmanj kritično izmed izpostavljenih in ga zato uvršča na zadnje mesto 9-mestne lestvice največjih groženj računalništva v oblaku.

Zlonamernost osebja ponudnikov – grožnja tega, da zlonamerno, nezadovoljno ali neetično osebje na strani ponudnika oblaka ali njegovih podizvajalcev lahko dostopa do podatkov in procesov naročnika. Navadno naročnik nima vpogleda v to, kakšne varnostne kontrole uporablja ponudnik, kakšne ravni pravic ima osebje, ki vzdržuje infrastrukturo računalništva v oblaku, in tudi ne v prostore, kjer se ta infrastruktura nahaja. CSA to tveganje uvršča na 6. mesto 9-mestne lestvice največjih tveganj računalništva v oblaku.

Neznana tveganja predstavljajo vsakršno moteno delovanje in nepooblaščen dostop do procesov ali podatkov naročnika zaradi netransparentnosti, odsotnosti varnostnih ukrepov, ki jih imajo uveljavljeni ponudniki računalništva v oblaku. Ponudniki večinoma to označujejo za poslovno skrivnost ali konkurenčno prednost, vendar to pravzaprav prispeva k manjši transparentnosti in stanovalec ne ve, kako je poskrbljeno za varnost in če jo ponudnik dejansko zagotavlja.

	Nivo tveganja*	
Vrsta tveganja	Leto 2010	Leto 2013
Odtekanje podatkov	5	1
Izguba podatkov	5	2
Ugrabitev storitev in podatkov	3	6
Ranljivi programski vmesniki	4	2
Zloraba in nezaželena uporaba računalništva v oblaku	7	1
Zlonamerno osebje ponudnikov	6	3
Skupne tehnološke ranljivosti	9	4

** nivo 1 = največje tveganje, nivo 9 = najmanjše tveganje*

Slika 2.5: Razvrščanje največjih tveganj po raziskavah CSA v letu 2010 in letu 2013

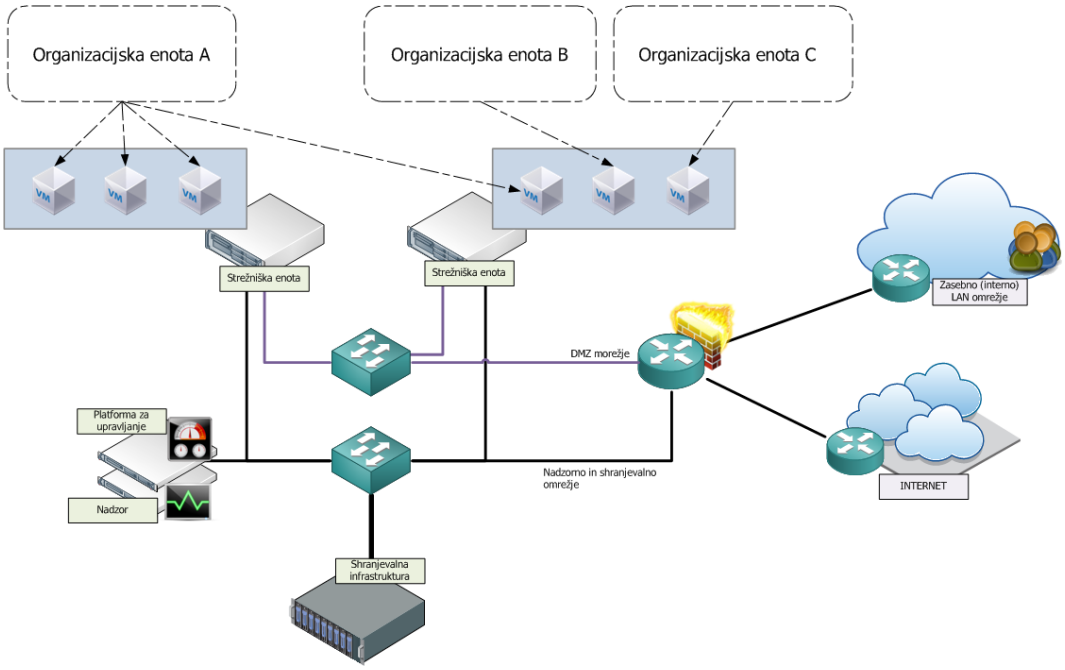
Poglavje 3

Varen prehod v zasebni oblak

3.1 Gradniki infrastrukture zasebnega oblaka

Za lažjo predstavo tega, na katere dele zasebnega računalništva v oblaku se bomo osredotočali, je vsekakor smiselno opisati posamezne komponente, ki nastopajo v opazovanem ekosistemu. Komponente so naslednje:

- varnostna politika in standardi dobrih varnostnih praks,
- fizična lokacija zasebnega oblaka,
- strežniška infrastruktura,
- mrežna infrastruktura,
- podatkovna infrastruktura,
- upravljavska infrastruktura,
- aplikacijska varnost.

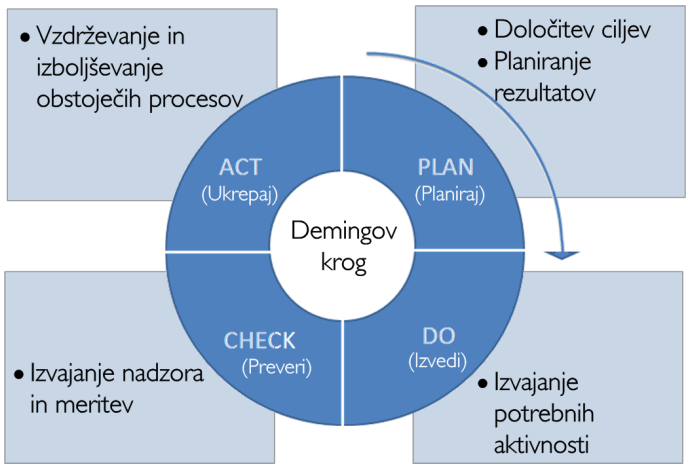


Slika 3.1: Diagram primera zasebnega oblaka

3.2 Priprava načrta za prehod v zasebni oblak

Za izgradnjo varnega zasebnega oblaka in varen prehod vanj potrebujemo v izhodišču dober načrt in predvsem dober pregled nad vsemi uporabniškimi potrebami. Tu govorimo tako o potrebah po funkcionalnosti in računskih virih kot tudi o varnostnih zahtevah pri obdelavi in shranjevanju podatkov, katerim moramo zadostiti na podlagi varnostne politike organizacije, posebnosti posameznega poslovnega področja, regulacij in zakonodaje glede varstva osebnih podatkov, ki velja za Slovenijo in Evropsko unijo.

Sama priprava in izvedba naj temeljita na procesnem pristopu **PDCA** [7] *(Plan, Do, Check, Act)* oz. "planiraj – izvedi – preveri – ukrepaj", ki ga uvajajo tudi že nekateri standardi, kot so *ISO 9001*, *ISO 27001*, *ITIL* itd.



Slika 3.2: Demingov krog

Skrbno načrtovanje varnosti zasebnega oblaka zajema varnost fizične lokacije in opreme, varnost računske infrastrukture, varnost omrežne infrastrukture, varnost shranjevalne infrastrukture, varnost upravljavske in avtomatizacijske platforme, ki upravlja zasebni oblak [8]. Četudi se organizacija odloči samo za najem zasebnega oblaka ali storitev, ki so s tem povezane, je s ponudnikom storitev računalništva v oblaku smiselno skleniti pogodbo, ki jasno opredeli varnostne vidike vse najete infrastrukture in dogovor o ravni storitve (SLA).

3.2.1 Osnovna načela varnosti in dobrih praks

Osnovna načela in izhodišča, ki jih lahko uporabimo za pripravo infrastrukture zasebnega oblaka in prehoda vanj [9]:

- **podvojenost komponent** – predpostavljamo, da kateri koli element zasebnega oblaka lahko odpove (tako varnostno kot funkcionalno), zato imamo pri načrtovanju v mislih, da kot celota ne sme biti kritično odvisen od posameznih sestavnih delov in bo deloval kljub napakam. Če imamo na razpolago dovolj virov, naj bodo ti porabljeni tako, da so določene komponente podvojene oziroma ne predstavljajo kritične točke v primeru odpovedi (angl. single point of failure),

- **načelo najmanjših pravic** – pri načrtovanju sistema uporabljamo pravilo, da za izvedbo določenega opravila in funkcije dodeljujemo najmanjše pravice dostopa, ki to izvedbo še omogočajo. Pravilo velja tako za računske kot tudi človeške vire in s tem zunanje podizvajalce. Na ta način poskrbimo, da morebitne (varnostne) napake ne morejo ogroziti delovanja in varnosti večjega dela zasebnega oblaka in njegovih stanovalcev,

- **preprostost** – osredotočimo se na enostavnost postavitve tako, da ne uvajamo konceptov in tehnologij, ki jih ne potrebujemo oziroma nimamo ustreznih virov za njihovo vzdrževanje. Vsi tovrstni koncepti in tehnologije lahko povečajo kompleksnost našega zasebnega oblaka, kar lahko pomeni ozko grlo tako pri vzdrževanju kot tudi delovanju celotnega zasebnega oblaka, ko pride do težav,

- **varnost v plasteh** – ker lahko posamezni gradniki zasebnega oblaka odpovejo, uporabljamo v kritičnih delih zasebnega oblaka več med seboj neodvisnih preventivnih mehanizmov hkrati. Uporabimo lahko na primer požarno pregrado in pravila prepuščanja protokola IP na požarni pregradi ali pa dodatno uporabimo seznam za kontrolo dostopa (angl. access control list, v nadaljevanju ACL) na posameznih vratih omrežnega stikala,

- **segmentacija stanovalcev/storitev** – kolikor je le mogoče upoštevamo izolacijo in gradimo storitve v "silosih" namenjene zgolj določeni skupini stanovalcev oziroma določeni skupini storitve.

3.2.2 Skladnost in zakonodaja

Informacijska varnost (angl. information security) pomeni varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, spremembo ali uničenjem, ki lahko ogrozijo poslovanje. Ko govorimo o informacijski varnosti, je vredno izpostaviti pojem "skladnosti". Tako je

določen informacijski sistem, del njega ali celoten poslovni proces itd. usklajen z nekimi preverjenimi, že uveljavljenimi standardi in predpisi delovanja oziroma obratovanja. Skladnost informacijske varnosti informacijskih sistemov z določenimi standardi navadno narekuje zakonodaja, interna politika organizacije ali celo pravila specifične gospodarske panoge (npr. bančni, zavarovalniški sektor). Presojo navadno naredijo ustrezni pooblaščeni zunanji revizorji, ki izdajo poročilo o skladnosti oziroma potrdilo, da je določen poslovni sistem skladen z določenim standardom.

Obstaja več že uveljavljenih dobrih praks, ki zajemajo tudi informacijsko varnost, varovanje podatkov in sistemov IT za izpolnitev osnovnih teženj informacijske varnosti po zagotavljanju zaupnosti, neokrnjenosti in razpoložljivosti informacijskih sistemov in njegovih dobrin. Največkrat se na tem mestu navaja predvsem:

- **ITIL** (angl. IT infrastructure library), ki predstavlja zbirko knjig z napotki in opisi za uvajanje in kakovostno izvajanje storitev IT, ki temeljijo na uporabi informacijske tehnologije,
- **CoBIT** (angl. Control Objectives for Information and related Technology), ki predstavlja zbirko nadzornih ciljev za upravljanje informacijske tehnologije. Zbirka delno pokriva in vključuje tudi ITIL, ISO 27002 in druge,
- skupino **ISO 27000** standardov, ki se nanašajo prav na informacijsko varnost. Iz te skupine je vredno omeniti ISO 27001, ki je nekakšen kodeks upravljanja in varovanja informacij, po katerem je možno podjetje/poslovni proces certificirati oziroma dobiti potrdilo o skladnosti po ustrezno prestani zunanji presoji.

ENISA *(European Union Network and Information Security Agency)* je novembra 2014 izdala EU strategijo certificiranih standardov za računalništvo v oblaku [10], v kateri jasno in nazorno razloži, da nobeden od trenutno uveljavljenih varnostnih standardov in okvirjev certifikacijskega postopka

ni narejen za certificiranje storitev računalništva v oblaku. Tako dopušča možnost souporabe določenih že uveljavljenih shem certificiranih standardov (PCI DSS, ISO 27001/2, ISO 20000 (ITIL), CSA Open Certification Framework, Eurocloud Star Audit, FISMA, ISACA COBIT ...) na čim bolj vitek (angl. lean) in cenovno dostopen način, ki vključuje tudi možnost samo-revizije po principu CSA Open Certification Framwork (Level 1 - CSA STAR) standarda[11] v nastajanju.

CSA je za ponudnike storitev računalništva v oblaku izdala t. i. Cloud Contol Matrix[12], v nadaljevanju CCM, pregledno matriko vseh uveljavljenih varnostnih standardov, regulacij in kontrol posameznih standardov. Je trenutno (september 2014) daleč najbolj obsežena kontrolna tabela, ki prikazuje, kako se zahteve in kontrole posameznih standardov med seboj prekrivajo in dopolnjujejo.

ENISA podaja mnenje, da če je potrebna certifikacija storitev računalništva v oblaku, je to certifikacija na nivoju skladnosti z varstvom podatkov (angl. data protection) [10].

Ko govorimo o računalništvu v oblaku, ne moremo mimo ključnega vprašanja, ki zadeva tudi zakonodajo, in to je predvsem, kje se nahajajo podatki ter kdo in na kakšen način z njimi upravlja; torej, ali so podatki v oblaku na varnem. Primarno govorimo tukaj o osebnih podatkih, kamor spadajo vsi podatki, ki se nanašajo na določenega ali določljivega posameznika.

Znotraj Evropske unije mora vsaka organizacija, ki ima/obdeluje kakršne koli osebne podatke, biti skladna z direktivo *Data Protection Act/European Data Protection Directive 95/46/EC* [13] oziroma vsebinsko ustreznim zakonom na nivoju posamezne članice EU. Varovanje osebnih podatkov je v Sloveniji pravno urejeno z Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 94/2007 — uradno prečiščeno besedilo; v nadaljevanju ZVOP-1) [14], ki ga je na tem mestu vredno izpostaviti in upoštevati, ko najemamo storitve računalništva v oblaku ali vzpostavljamo svoj zasebni oblak, ne glede na

to, ali bomo njegove storitve tržili dalje oziroma dajali v souporabo tretjim osebam.

Na temo računalništva v oblaku in na podlagi slovenske zakonodaje (Zakona o varstvu osebnih podatkov) je Informacijski pooblaščenec Republike Slovenije skupaj s CSA Slovenija, Slovenskim inštitutom za revizijo, slovenskim odsekom ISACA izdal smernice z naslovom *"Varstvo osebnih podatkov in računalništvo v oblaku"*. Dosegljive so na spletnih straneh Informacijskega pooblaščenca RS [15].

> "*Namen smernic je podati enotne kontrolne točke, s pomočjo katerih bodo lahko tako uporabniki kot nadzorni organi sprejemali bolj informirane odločitve glede uporabe in nadzora računalništva v oblaku v delu, ki se nanaša na obdelavo osebnih podatkov, ponudnikom storitev računalništva v oblaku ter iniciativam za varnost in certificiranje tovrstnih storitev pa naj bi ponudile napotke za nadaljnji razvoj s ciljem skladnosti z zakonodajo o varstvu osebnih podatkov.*"[15]

Zap.št.	Kontrolna točka	DA	NE	N	P	Smernice za izpolnitev	Zakonska referenca
Obdelava osebnih podatkov - splošno							
1	Naročnik razpolaga s pravno podlago za obdelavo osebnih podatkov.	☐	☐	x		Naročnik mora razpolagati s pravno podlago (npr. privolitev posameznika ali podlaga v zakonu) za obdelavo osebnih podatkov, da sploh lahko obdeluje in posreduje osebne podatke (še preden se torej odloči za uporabo storitev računalništva v oblaku). Pravne podlage, kot so npr. privolitev posameznika ali podlaga v zakonu, opredeljujejo 8., 9., 10. člen ZVOP-1.	8., 9., 10. člen ZVOP-1
						Naročnik mora v vsakem trenutku vedeti, katere kategorije osebnih podatkov iznaša v oblak; to lahko predstavlja katalog zbirke osebnih podatkov, podatkovni model.	

Slika 3.3: Primer dela kontrolnega seznama za varstvo osebnih podatkov v računalništvu v oblaku [15]

Zakonodajalec lahko za določene segmente uporabnikov celo dodatno predpiše obvezno skladnost z določenimi varnostnimi standardi in tako zasledimo, da Banki Slovenije skladno z Zakonom o bančništvu (Uradni list RS,

št. 83/2004) [16] narekuje, da mora vsaka banka v Sloveniji za opravljanje bančnih oz. drugih finančnih storitev upoštevati slovenska standarda *SIST BS 7799-2:2003* in *SIST ISO/IEC 17799:2003*. Gre za starejšo različico varnostnih standardov ISO 27001 in ISO 27002.

3.3 Fizična infrastruktura oblaka

Varnostne informacijske infrastrukture zasebnega oblaka na najnižji ravni temeljijo na nadzoru fizičnega dostopa do fizičnih komponent zasebnega oblaka; te ravni ne gre podcenjevati. V primeru gradnje lastnega zasebnega oblaka v prostorih organizacije se pravila varovanja fizičnega prostora oziroma podatkovnega centra, v katerem gradimo zasebni oblak, ne razlikujejo od pravil in protiukrepov, ki jih uporabljamo za varovanje ostale strežniške in mrežne infrastrukture. Govorimo o istih fizičnih gradnikih, ki v infrastrukturi nastopajo in so izpostavljeni istim grožnjam.

Nepooblaščen fizični dostop ali dostop neprimerno usposobljenega osebja predstavlja neposredno grožnjo samemu delovanju zasebnega oblaka in varnosti podatkov, ki se znotraj oblaka hranijo in obdelujejo, posredno pa ogroža poslovanje organizacije, njeno premoženje in tudi njeno dobro ime.

V ta namen uvajamo naslednje varnostne kontrole [17], ki so tako dobre in s strani določenih regulatorjev/standardov celo zahtevane prakse:

- **fizično varovanje objektov in prostorov**; predvsem prepovedan vstop nepooblaščenim osebam v podatkovno središče,

- **fizična kontrola dostopa** predstavlja sledenje temu, kdo (seveda izmed pooblaščenih oseb) in kdaj je v času obratovanja bil fizično prisoten v podatkovnem centru oziroma je izvajal določene operacije na fizični opremi. Tovrsten podatek dostikrat pomaga pri iskanju korelacije z določenim incidentom, ki je lahko povezan tako z neprekinjenim poslovanjem oziroma motenim procesom kot tudi varnostnim incidentom,

- **alarmni sistemi** – dodatno varovanje prostorov, v katerih se nahaja vitalna in kritična infrastruktura, z alarmnimi sistemi s hitrim odzivom intervencijske ekipe,
- **video nadzor** – vsi vstopi in opravila, tudi pooblaščenih oseb in izvajalcev, se v podatkovnem centru dodatno beležijo s sistemom video nadzora.

Podatkovni center in ostala kritična infrastruktura sta izpostavljena tudi ostalim nezaželenim vplivom/nevarnostim, ki niso neposredno povezane s človeškim faktorjem, kot so npr. pregrevanje prostora in požar, izpad primarnega električnega napajanja podatkovnega centra, poplave in vsi ostali vplivi iz okolja. V ta namen je treba vsekakor uvesti tudi ustrezne protiukrepe:

- **zaznava in gašenje požara** zato, da lahko, ko pride do vžiga zaradi mehanske/tehnične napake ali iz malomarnosti osebja, pravočasno izoliramo mesto požara oziroma ustrezno obvestimo odgovorno/dežurno osebje, ki stopi v akcijo skladno s postopki ravnanja v primeru tovrstne grožnje,
- **podvojeno električno napajanje** zato, da v primeru izpada primarnega vira napajanja podatkovnega centra lahko računalniška infrastruktura nemoteno obratuje preko sekundarnega vira napajanja,
- **nadzor nad temperaturo in vlago v prostoru** za zagotavljanje in spremljanje optimalne izrabe energije tako za ohlajanje prostora kot neprekinjeno delovanje računalniške opreme v prostoru. Proaktivno spremljanje atmosfere prostora lahko prepreči celo požar, še predno do njega pride.

Pri gradnji zasebnega oblaka se srečamo tudi s postavitvenim modelom, v katerem infrastruktura zasebnega oblaka ni v prostorih, ki jih upravlja organizacija/lastnik, ampak zunanji ponudnik kolokacijskih storitev (najem prostora v podatkovnem centru) ali celo zunanji ponudnik storitev računalništva

v oblaku, ki nudi storitev zasebnega oblaka. V primeru tovrstnega najema je s stališča varnosti primerno skleniti tako naročniško pogodbo in SLA, kjer je opredeljeno tudi ustrezno varovanje fizične infrastrukture zasebnega oblaka in redno revidiranje tega s strani zunanjega neodvisnega presojevalnega organa, ki je za to pooblaščen.

3.4 Strežniška infrastruktura

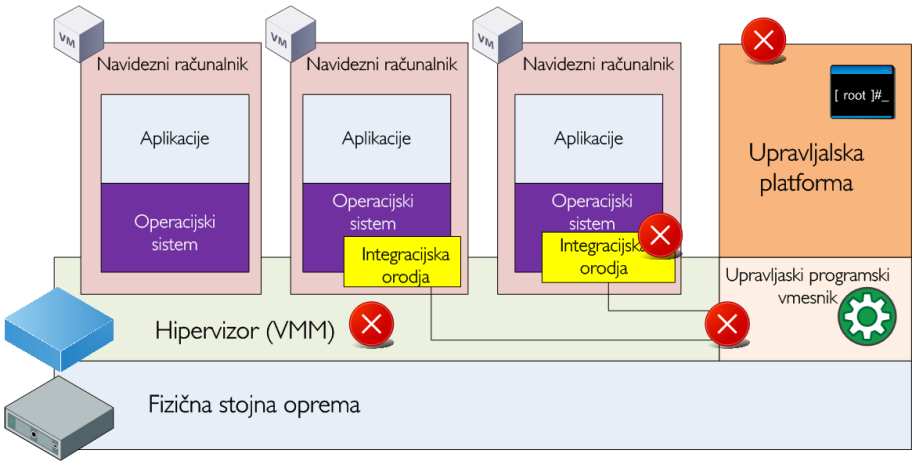
Strežniška infrastruktura nudi računske in pomnilniške vire zasebnega oblaka, ki jih porazdelimo med uporabnike in uporabniška okolja v organizaciji. Na kakšen način razdelimo strežniško infrastrukturo med poslovne enote v podjetju, je stvar samega načrta in zajema potrebe posameznih aplikacij, različnih poslovnih enot, ki jih selimo v zasebni oblak.

Ključno tveganje na nivoju računske infrastrukture, ne glede na to, da gre za zasebni oblak, še vedno obstaja, sploh ko govorimo o mehanizmih sobivanja, kot je izolacija posameznih navideznih računalnikov na nivoju virtualizacije.

3.4.1 Ranljivost hipervizorjev in virtualizacijskega okolja

Pred uporabo virtualizacije je infrastrukturni sklad sestavljala strojna oprema, operacijski sistem, aplikacije znotraj operacijskega sistema in komponenta za upravljanje celotne infrastrukture. Z uvedbo virtualizacije infrastrukturni sklad razširimo z vmesnim nivojem hipervizorja, komponento virtualiziranega omrežja, vmesniki za komunikacijo posameznih navideznih računalnikov s hipervizorjem itd. Vse te nove komponente predstavljajo nova tveganja za napade, ki bi ogrozili delovanje posameznega navideznega računalnika oziroma omogočili nepooblaščene dostope med navideznimi računalniki in posredno tudi do podatkov uporabnikov znotraj.

Tako imamo v splošnem 4 komponente (komponente in njihova implementacija se seveda razlikujejo od virtualizacijske plaforme), ki predstavljajo naslednja tveganja:



Slika 3.4: Ranljive točke virtualizacijskega okolja

- Komponenta **uporabniški upravljavski vmesnik API** (angl. Client Managment API) znotraj navideznega računalnika, ki komunicira s programskim vmesnikom za upravljanje hipervizorja. Poznani so napadi, kot so skok iz navideznega računalnika (angl. VM jumping), skok v pomnilniški prostor drugega navideznega računalnika (in s tem tudi stanovalca) in napad na sam hipervizor v obliki ohromitve storitve (angl. hypervisor DoS attacks).

- Komponenta **upravljalski vmesnik hipervizorja** (angl. Host managment API) je predvsem ranljiva na ohromitve celotnega hipervizorja in s tem vseh navideznih računalnikov, ki se izvajajo na tem fizičnemu strežniku.

- Komponenta **hipervizor** (angl. Hypervisor oziroma pojavlja se tudi z imenom *'Virtual Machine Monitor'*) kot aplikacija, ki teče v privilegiranem načinu, neposredno upravlja s fizičnimi strojnimi komponentami strežnike infrastrukture in skrbi za virtualizacijo naprav, upravljanje s

pomnilnikom, izolacijo in razvrščanjem procesov v centralni procesni enoti. Ena od glavnih značilnosti hipervizorja je seveda tudi prestrezanje programskih inštrukcij navideznega računalnika, da operacijski sistemi znotraj navideznega računalnika ne razlikuje glede na to, ali tečejo v virtualiziranem ali nevirtualiziranem okolju

- Komponenta **upravljavska platforma** (angl. VM management infrastracture) predstavlja predvsem vmesnik za upravljanje računskega dela infrastrukture, hipervizorja in posredno avtomatizacijo in orkestracijo tega z ostalimi komponentami zasebnega oblaka. V večini primerov je implementacija izvedena kot "REST" spletni programski vmesnik (angl. Application Programming Interface – API), preko katerega orkestracijo izvajajo ostale programske komponente za upravljanje celotne oblačne platforme. Ker mora tovrstna komponenta biti dosegljiva preko omrežja IP, je izpostavljena predvsem potencialnemu neprivilegiranemu dostopu oziroma zavrnitvi storitve pri porazdeljenem napadu (DDoS).

Prve resnejše ranljivost hipervizorjev v primeru uporabe polne virtualizacije na sistemih x86 so bile predstavljene že leta 2006 na varnostni konferenci Black Hat USA [18], kjer je bil predstavljen "Blue Pill/Subvirt" [19] napad, ki demonstrira implementacijo zlonamernega hipervizorja nad obstoječi hipervizor ter tako prestreza in upravlja navidezni računalnik, ki nima vednosti o zlonamerni kodi.

Verjetnost ranljivosti programske kode hipervizorjev je v praksi zelo nizka, ker je virtualizacija strežnikov bila že kar ustaljena praksa IT še pred računalništvom v oblaku in je programska koda navadno že temu primerno predtestirana in preizkušena. Tako ocenjuje tudi CSA [6]. Ne gre pa podcenjevati tovrstnih ranljivosti, ker ob njihovi zlorabi lahko potencialno napadalec dostopa do navideznega računalnika, podatkov ter vseh ostalih omrežnih virov, ki so priključeni v navideznem računalniku.

Nekaj primerov zanimivih odkritih ranljivosti iz zgodovine:

- *"VMware Cloudburst"* [20] je bil predstavljen na konferenci Black Hat USA 2009, kjer je hipervizor ponujal navideznemu računalniku uporabo določenih 3D grafičnih komponent, ki pa so omogočale uhajanje pomnilnika (angl. memory leak) ter dostop in pisanje izven pomnilniškega prostora, namenjenega navideznemu računalniku. Na ta način je bilo možno obiti izoliranost in se sprehoditi po pomnilniškem prostoru hipervizorja ali celo drugega navideznega računalnika.

- *"Virtunoid: Breaking out of KVM"* [21] je ranljivost, odkrita na odprtokodni implementaciji virtualiziranega okolja KVM/Qemu-KVM. V implementaciji emulacije upravljanja z napajanjem (angl. power management) je bila odkrita slabo napisana koda za odstranitev "hotplug naprav" *(naprava, ki jo je možno med delovanjem sistema poljubno priklapljati in odklapljati)* iz navideznega računalnika, ki je omogočala tako sesutje dotičnega navideznega računalnika kot tudi pridobitev privilegiranega dostopa na nivoju strežnika, ki poganja hipervizor in navidezne računalnike.

- Ranljivost, odkrita leta 2011, prav tako na hipervizorju proizvajalca VMware, ki je omogočala na emulaciji mrežne naprave *Intel e1000* z enim od gonilnikom VMware, da je napadalec lahko obšel nastavljene paketne filtre za varovanje [22].

- Leta 2012 odkrita ranljivost *"VMDK Has Left The Building"* [23] kaže na pomanjkljivost v načrtu tega, kako okolje VMware ESX upravlja z diskovnimi polji navideznih računalnikov. V datoteko VMDK, ki je tekstovna datoteka z opisom komponent, nastavitev navideznega računalnika in diskovnih polj, je bilo mogoče dopisati katerokoli datoteko hipervizorja ali priključeno diskovno napravo, ki je hipervizor oziroma posledično kateri koli drug navidezni računalnik ne uporablja, jo tako "priključiti" v navidezni računalnik in dostopati do vsebine. Nevarnost je bila toliko večja, ker so določeni ponudniki tovrstnih oblačnih

storitev, temelječih na okolju ESX, omogočali, da si je stanovalec sam naložil sliko navideznega računalnika in prenesel svojo VMDK datoteko v okolje. VMWare je to varnostno luknjo ob izidu novih popravkov za ESX/ESXi seveda že odpravil, vendar bojazen za podobne (še neodkrite) varnostne luknje ostaja.

3.4.2 Priporočila za izboljšanje varnosti virtualizacijskega okolja

Ne glede na izbrano vrsto virtualne tehnologije, ki bo poganjala računske vire, je smiselno v skladu z načrtom implementacije zasebnega oblaka pregledati priporočila proizvajalca tehnologije in skladnost s strojno in programsko opremo, ki ju bomo uporabljali. Načrtovanje in utrjevanje strežniške infrastrukture je priporočeno uskladiti z dobrimi praksami in priporočili proizvajalca, standarda in regulatorja. Tovrstna priporočila so na voljo tako za komercialna virtualna okolja, npr. proizvajalca VMware [24], Microsoft Hyper-V [25], kot odprtokodna virtualna okolja in platforme KVM [26], XEN [27, 28].

Za najboljšo izolacijo med stanovalci je smiselno uporabiti naslednje varnostne protiukrepe [31], ki jih med drugim tudi predlaga NIST v svoji publikaciji NIST 800-125 [29] in NIST 800-144 [30], ter PCI-DSS [32] za npr. skladnost s PCI-DSS standardom:

- skrbna priprava načrta varnosti virtualizacijske rešitve za polno virtualizacijo pred samo implementacijo,
- dodatno utrjevanje izbrane infrastrukture na ravni navideznih strežnikov, navideznih omrežij in upravljavske platforme po priporočilih proizvajalca,
- uporaba zadnjih popravkov na programski opremi hipervizorja in sledenje popravkom s strani proizvajalca,

- izklop komunikacije med navideznimi računalniki preko VMCI komponente *(specifično za VMware produkte)*,
- stalno preverjanje skladnosti z varnostnimi nastavitvami,
- izklop nepotrebnih funkcionalnosti računske/virtualizacijske rešitve, ki bi lahko ogrožale varnost posameznih stanovalcev,
- spremljanje porabe računalniških virov med stanovalci in preprečevanje motenj, ki bi lahko nastale pri (napačni) uporabi računalniških virov posameznega stanovalca oziroma navideznega računalnika,
- natančna pravila za omejevanje upravljavskega dostopa do posameznih funkcij zasebnega oblaka in posameznih računalniških virov,
- centralizirano spremljanje upravljavskih dostopov in spremljanje porabe vseh računskih virov,
- fizično ločevanje stanovalcev na računalniški infrastrukturi v primeru zahtevnejših okolij oziroma ločitev glede na namembnost. Primer dobre prakse je, ko sestavlja zasebni oblak računalniška infrastruktura z več fizičnimi strežniki in se znotraj zasebnega oblaka izvaja več različnih okolij *(npr. produkcijsko, razvojno itd)*, da okolja glede na namembnost razporedimo po fizičnih strežnikih,
- omejen dostop do upravljavske platforme in spletnih vmesnikov za upravljanje zasebnega oblaka; preko ene vhodne točke z uporabo tehnologij VPN oziroma iz pooblaščenih lokacij/omrežij znotraj organizacije.

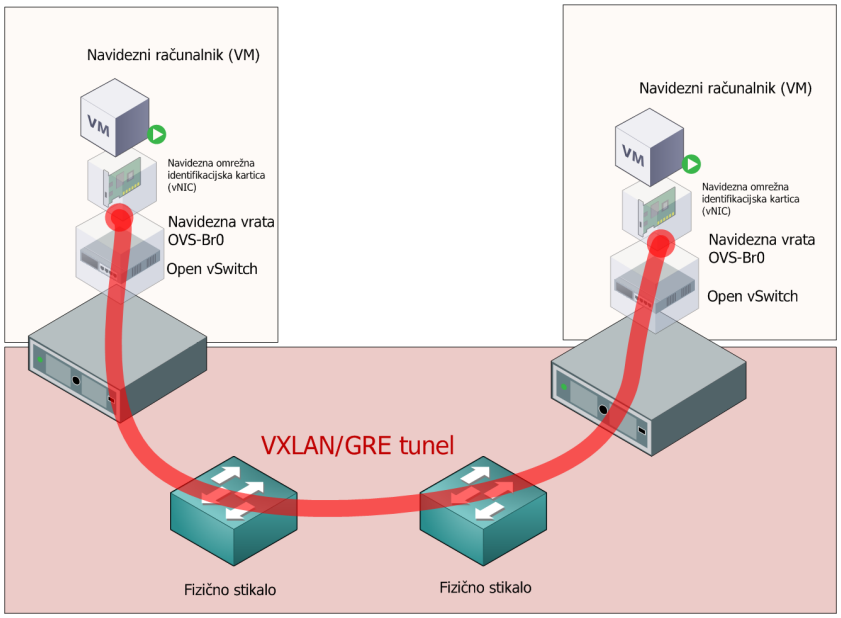
3.5 Omrežje in komunikacijske poti

Omrežna infrastruktura znotraj zasebnega oblaka nudi storitve povezljivosti med navideznimi računalniki in ostalimi zasebnimi (internimi) omrežji organizacije in tudi možnost povezljivosti v javna omrežja (internet, oddaljena omrežja, povezljivost v zunanje oblake itd.). Izgradnja omrežja (in omrežij)

zasebnega oblaka se prav dosti ne razlikuje od do sedaj znanih in uveljavljenih principov izgradnje klasičnega omrežja protokola IP. Računalništvo v oblaku na nivoju virtualizacije omrežja prinaša določene (nove) koncepte, ki predvsem omogočajo lažjo orkestracijo, upravljanje in do neke mere tudi fleksibilnost, ki bi jo morda znotraj oblaka potrebovali, sploh ko določeno storitev računalništva v oblaku oziroma navidezni računalnik prenašamo tako med različnimi hipervizorji in med različno strežniško strojno opremo kot tudi geolokacijsko med različnimi podatkovnimi centri itd. Pri virtualizaciji omrežja v oblaku se tako srečamo z (novimi) koncepti.

- **Prekrivna omrežja** (angl. Overlay (Virtual) Networking), v katerih na obstoječem omrežju protokola IP gradimo kompletno novo omrežje, ki povezuje navidezne računalnike in ustrezne mrežne komponente, kot so požarne pregrade, usmerjevalniki, stikala, naprave za uravnoteženje omrežnih obremenitev (angl. load balancing) itd. Za novo nastalo prekrivno omrežje niso pomembne podrobnosti fizičnega omrežja. Tovrstna topologija "omrežja nad omrežjem" ni nov koncept in jo lahko srečamo že pri povezovanju prostranih omrežij (angl. Wide Area Network – WAN) z uporabo protokola *MPLS/VPN*. Za izgradnjo tovrstnih omrežij danes obstaja že nekaj uveljavljenih standardnih protokolov, kot so VXLAN *(Virtual Extensible LAN)*, (NV)GRE *(Network Virtualization using Generic Routing Encapsulation)* in STT *(A Stateless Transport Tunneling Protocol for Network Virtualization)*. Standardi se med razlikujejo po različnih tehnikah enkapsulacije, ampak v osnovi delujejo na zelo podoben način. Določene napredne storitve virtualizacije (mobilnost navideznih računalnikov/storitev) potrebujejo povezljivost znotraj iste kolizijske domene (angl. ethernet broadcast domain). Ta zahteva lahko povzroči rast tovrstnega Ethernet omrežja do neobvladljivih razsežnosti, tako s strani upravljanja kot potencialnih ranljivosti Ethernet nivoja, še zlasti ko se Ethernet omrežje razteza med dvema ali več podatkovnimi centri. Z uvedbo navideznih Ethernet omrežij VLAN (angl. virtual local area network) zmanjšamo tovrstne

kolizijske domene in povečamo izoliranost med posameznimi storitvami, ampak standard VLAN IEEE 802.1Q [33] *(standard, ki je navadno implementiran na vseh stikalih z podporo VLAN)* omogoča sobivanje samo 4096 tovrstnih ločenih omrežij. Sprva se to sliši "dovolj", ampak pri predpostavki, da vsak stanovalec vzpostavi vsaj eno svoje omrežje VLAN, lahko to predstavlja omejitev. Z uvedbo prekrivnih omrežij zgradimo omrežje stanovalcev na omrežju protokola IP ter odpravimo omejitev števila omrežij VLAN. Pridobimo pa tudi lastnost protokola IP, npr. usmerjanje in filtriranje naslovov IP. Glavna prednost je, poleg same izolacije, da protokol STP (angl. Spanning Tree Protocol) za odkrivanje zank (angl. ethernet loop) znotraj novega ethernet omrežja, ki lahko ob napačni konfiguraciji ali anomaliji v omrežju naredi tega nestabilnega, omejimo zgolj na stanovalčevo omrežje, ne da pri tem ogrozimo delovanje ostalih omrežij stanovalcev oblaka.



Slika 3.5: Primer prekrivnega omrežja s protokolom VXLAN

- **Virtualizacija omrežnih funkcij** [34] (angl. Network Function Virtualization) je koncept, s katerim klasične gradnike omrežja in omrežne

naprave preselimo v virtualizirano okolje oziroma virtualiziramo, da postanejo namenski navidezni računalniki, ki si delijo sistemske vire fizične strežniške infrastrukture skupaj z ostalimi navideznimi računalniki. Tukaj govorimo o gradnikih, kot so požarne pregrade, usmerjevalniki, mrežna stikala, naprave za pametno uravnovešanje prometa (angl. load ballancing), ki sestavljajo nova prekrivna omrežja. Bistvena prednost v primerjavi s klasičnimi fizičnimi omrežnimi napravami je seveda mobilnost tovrstne virtualizirane naprave, posledično tudi omrežij stanovalcev med hipervizorji znotraj oblaka. Seveda pa tukaj ne gre zanemariti tudi možnosti visoke razpoložljivosti tovrstne virtualizirane naprave, ki jo ponuja gruča hipervizorjev v oblaku.

- Koncept **programabilnosti omrežja** [35] (angl. software defined networking – SDN) predstavlja predvsem ločitev nadzorne ravnine (angl. control plane) od podatkovne ravnine (angl. data plane) mrežnih naprav. Tako vsi omrežni gradniki fizičnega omrežja in virtualizirane naprave postanejo programabilni s strani nadzorne naprave (angl. network controller), ki na vse mrežne gradnike naloži ustrezna pravila za posredovanje podatkov in zgradi topologijo novo nastalega omrežja na omrežju. Navadno vse mrežne komponente komunicirajo znotraj istega omrežja IP z nadzorno napravo in nad tem omrežjem potem zgradijo ustrezno topologijo po principu prekrivnih omrežij.

3.5.1 Tveganja na omrežnem nivoju

Grožnje in nevarnosti na omrežnem nivoju znotraj zasebnega oblaka ostajajo identične, kot jih poznamo v katerem koli drugem zasebnem omrežju. Tako ostajajo še vedno prisotne nevarnosti na sloju podatkovne povezave (na povezovalni plasti), kot na primer [36]:

- ponarejanje strojnega naslova MAC (angl. medium access control – MAC) in preplavljanje pomnilniškega prostora za strojne naslove MAC na stikalih,

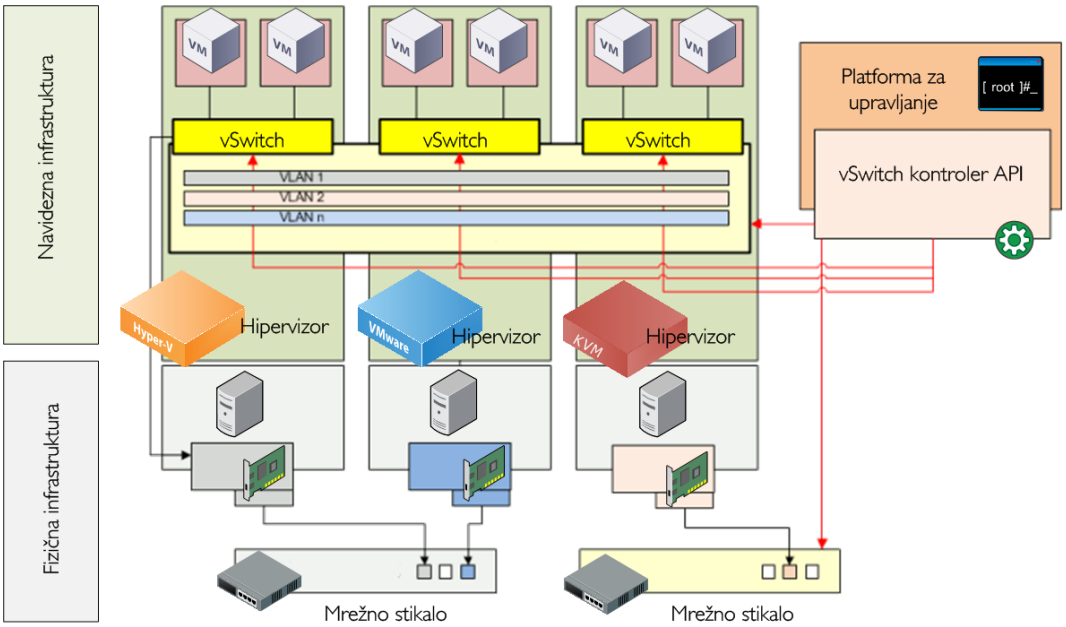
- ponarejanje zapisov ARP (angl. ARP spoofing) in preusmerjanje oziroma namerno prestrezanje komunikacijske poti,
- skok iz obstoječega omrežja VLAN v drugega (angl. VLAN hopping),
- napadi na protokol STP, ki posledično vplivajo na delovanje omrežja in povezljivost navideznih računalnikov s preostalim omrežjem.

Podobno pa velja tudi za omrežni nivo IP, kjer tako srečamo napade [37]:

- ponarejanje naslova IP (angl. IP spoofing), največkrat povezanega z napadi s preplavljanjem (angl. flood attacks) in posledično z zavrnitvijo storitve pri porazdeljenem napadu (DDoS),
- napadi na protokol DHCP (angl. DHCP attacks), pri katerih se napadalec predstavlja za strežnik DHCP (angl. DHCP server spoofing) v omrežju za dodeljevanje naslovov IP ali pa "izprazni" IP-naslovni prostor strežnika DHCP, namenjenega za dodeljevanje (angl. DHCP starvation),
- napadi, povezani s storitvijo DNS, ki izvaja preslikavo med domenskimi imeni in naslovi IP. Med bolj izpostavljenimi napadi je zastrupljanje predpomnilnika DNS (angl. DNS cache poisoning), pri čemer napadalec v predpomnilnik strežnika DNS podtakne lažna domenska imena,
- napadi na dinamične usmerjevalne protokole.

3.5.2 Priporočila za izboljšanje varnosti na omrežnem nivoju

Pri načrtu omrežne infrastrukture je tako kot že v poglavju prej ključnega pomena izolacija posameznih stanovalcev oziroma navideznih računalnikov tudi na omrežnem nivoju.



Slika 3.6: Primer infrastrukture izoliranega omrežja znotraj zasebnega oblaka

Pri gradnji zasebnega oblaka je možnih različnih topologij na podlagi različnih tehnologij, ki se lahko uporabljajo. Podobno kot pri načrtovanju varnosti računske infrastrukture, je priporočeno upoštevati priporočila proizvajalca mrežne opreme. Smiselno je stremeti k temu, da vsak stanovalec storitve zasebnega oblaka dobi logično ločeno omrežje LAN, ki je od ostalih stanovalcev in javnih omrežij ločeno na več ravneh. Večstanovalsko ločitev uporabnikov na omrežni infrastrukturi lahko zagotavljamo s kombinacijami fizične in logične ločitve v omrežju. Pri tem je vredno upoštevati naslednje metode in koncepte [30, 38]:

- znotraj navideznih omrežij virtualizacijske platforme uporabljati ločitev z navideznimi omrežji *(navadno vezano na proizvajalca oziroma uporabljeni tip virtualizacije)*,
- na fizični opremi posamezne naprave ločiti s tehnologijo navideznih LAN segmentov – VLAN *(IEEE 802.1Q)*,
- s strogim medsebojnim ločevanjem stanovalcev na povezovalni plasti

preprečujemo napade, kot so potvarjanje zapisov ARP (angl. ARP spoofing), napadi na tabele MAC na stikalih (angl. MAC spoofing) in ostale anomalije,

- stanovalce med seboj ločiti z namenskim požarnim zidom oziroma promet IP med dvema segmentoma stanovalcev usmeriti preko požarne pregrade, ki ima nameščena ustrezna varnostna pravila,
- stanovalci naj bodo od javnih omrežij *(interneta)* prav tako ločeni z namensko požarno pregrado,
- za ločevanje omrežij z najvišjo stopnjo varnostne nezdružljivosti uporabljamo fizično ločevanje lokalnih omrežij in fizično ločene vmesnike požarnih zidov v primerih, ko je omejena komunikacija med omrežji potrebna,
- ločitev fizičnih poti omrežja za upravljanje (angl. management network) in omrežja naprav za shranjevanje (angl. storage network) od ostale infrastrukture,
- utrjenost mrežnih naprav z izklopom nepotrebnih storitev,
- močno kriptografsko zaščitene povezave IPSec VPN prek omrežja internet med zasebnim oblakom in oddaljenim uporabniškim omrežjem,
- varno usmerjanje omrežnega prometa protokola IPv4 in IPv6; uporaba overjenih usmerjevalnih protokolov prek zaupanja vrednih omrežij in filtriranje usmerjevalnih informacij za preprečevanje kraje prometa,
- nadzor nad izvornimi naslovi IP s seznami za kontrolo (ACL) in mehanizmi, kot je uRPF (angl. unicast reverse path forwarding),
- omejevanje dostopa do funkcij za upravljanje omrežne infrastrukture,
- stalno preverjanje ustreznosti in prisotnosti nastavitev varnostnih protiukrepov v omrežni infrastrukturi,

- dejavno spremljanje delovanja in morebitnih anomalij ter uporaba sistema za beleženje in upravljanje z varnostnimi incidenti.

3.6 Podatki in shranjevalna infrastruktura

Shranjevalna infrastruktura v zasebnem oblaku nudi računalniški infrastrukturi vire, s katerimi zagotavljamo tako delovno kapaciteto za uporabniške podatke kot podporo storitvam za izvajanje rezervnih kopij podatkov.

Shranjevalna infrastruktura je lahko v zasebnem oblaku implementirana na več načinov. Od najenostavnejše/preproste postavitve, ko računska infrastruktura izrablja diskovna polja fizičnih strežnikov, na katerih tečejo navidezni računalniki, do shranjevalne infrastrukture, ki je dosegljiva preko omrežja. V tem primeru govorimo o ločenih namenskih napravah, ki preko različnih protokolov nudijo računalniški infrastrukturi omrežne shranjevalne vire. Govorimo navadno o namenskih napravah, kot so omrežje pomnilniških naprav (angl. storage area network – SAN) in omrežna diskovna polja (angl. network attached storage – NAS), ki lahko nastopajo tudi v virtualizirani obliki.

Strežniška infrastruktura in navidezni računalniki, ki tečejo na njej, lahko navadno uporabljajo več tipov dostopa do podatkov na oddaljeni shranjevalni infrastrukturi, ki je lahko tako centralizirana ali razpršena v omrežju.

- **Dostop na nivoju blokov** (angl. block level storage), pri katerem hipervizor oziroma navidezni računalnik dostopa do ustrezne shranjevalne enote (angl. logical unit number – LUN) na napravi SAN. Dostop je na nivoju blokov in ne datotek. Sama naprava SAN nima nobene vednosti o podatkih na pomnilniškem polju. Za komunikacijo z napravo SAN je mogoče uporabiti več protokolov. Med najbolj razširjene sodijo:
  - FC (angl. Fiber Channel), ki predvideva ločeno omrežje in ustrezna FC omrežna stikala za povezovanje,

  - FCoE (angl. Fiber Channel Over Ethernet), ki omogoča kombiniranje protokola FC skozi obstoječa ethernet omrežje in stikala, ki podpirajo tako FC kot ethernet povezljivost,
  - iSCSI (angl. Internet Small Computer System Interface), ki deluje na mrežnem protokolu IP in ponuja fleksibilnost, če navidezni računalnik in shranjevalna omrežna enota nimata direktne neposredne povezave [39],
  - AoE (angl. ATA Over Ethernet).

- **Dostop na nivoju datotek** (angl. file level storage), pri katerem navidezni računalnik dostopa neposredno do datotek na shranjevalni enoti oziroma napravi NAS. Navadno se uporablja pri tovrstni komunikaciji enega od protokolov za skupno rabo, kot so na primer SMB, NFS, ZFS. Glavna prednost tovrstnega dostopa na nivoju datotek je seveda možnost, da lahko več navideznih računalnikov dostopa do istih datotek sočasno; to pa predstavlja tudi največjo nevarnost z vidika varnosti, in sicer v primeru ranljivosti katerega od komunikacijskih protokolov ali slabo nastavljenih nastavitev seznama za kontrolo dostopa na sami napravi NAS.

- **Dostop na nivoju objektov** (angl. object-based storage) je novejša oblika shranjevalne infrastrukture, ki prihaja v ospredje z razvojem računalništva v oblaku. Ta shranjevalni model je bolj storitveno orientiran in predvsem reši problem sočasnih dostopov pri pisanju več sočasnih uporabnikov. Vsa komunikacija je navadno realizirana na nivoju klicev *RESTful* API in z uporabo varnih protokolov SSL/TLS. Storitev običajno podatke oziroma datoteke shranjuje v obliki objektov v podatkovno skladišče, ki je navadno lahko razpršeno med več shranjevalnih virov. Tovrstna shranjevalna storitev je najbolj primerna za terciarno shrambo podatkov, ki je navadno bistveno počasnejša v primerjavi z dostopi na nivoju blokov ali datotek pri enotah SAN/NAS. Primer najbolj znane tovrstne rešitve v javnem oblaku je storitev Ama-

zon S3 [40], ki nudi javno dostopen programski vmesnik – API za dostop do podatkov. V zasebnem oblaku pa storitve, kompatibilne z Amazon S3 API, nudita npr. odprtokodna rešitev *Openstack Swift* [41] in *Ceph* [42], ki omogoča vse tri vrste dostopov na decentralizirani infrastrukturi v omrežju.

3.6.1 Priporočila za izboljšanje varnosti shranjevalne infrastrukture

Za zagotavljanje visoke varnosti podatkov morajo posamezne logične enote shranjevalne infrastrukture biti prav tako primerno izolirane; večstanovalska ločitev stanovalcev na shranjevalni infrastrukturi, ki si jo delijo. Ločitev je smiselno prilagoditi izbrani tehnologiji, arhitekturi in namenu shranjevalne infrastrukture. Predvsem slednje igra ključno vlogo pri tem, kako bomo zavarovali podatke na shranjevalni infrastrukturi, da ti ne bodo dostopni potencialnim sostanovalcem zasebnega oblaka ali bili celo izpostavljeni in vidni javnemu delu interneta. Tako je pri sami implementaciji smiselno upoštevati naslednje ukrepe:

- upoštevanje navodil in dobrih praks implementacije proizvajalca ustrezne shranjevalne infrastrukture, uporaba namenskih in izoliranih omrežij med shranjevalno infrastrukturo in hipervizorji ločeno od podatkovnega omrežja stanovalcev,

- v primeru uporabe centraliziranega sistema, kot je npr. SAN, k tej ločitvi dodatno pripomore nadzor dostopa shranjevalnega polja na podlagi priključenih virtualizacijskih strežnikov na ravni omrežja SAN (“FC zoning”) ter pravila dostopa do shranjevalnih enot LUN glede na identiteto virtualizacijskih strežnikov na samem shranjevalnem polju [43, 44],

- pri novejših oblikah razpršene shranjevalne infrastrukture je v primeru, da je ta dostopna več stanovalcem, dobro dodatno poskrbeti, da je vsa

omrežna komunikacija kriptografsko zaščitena s protokolom SSL/TLS ali njemu sorodnimi,

- uporaba seznamov kontrole dostopov na več nivojih, še zlasti na shranjevalni infrastrukturi, ki omogoča sočasno uporabo več sostanovalcev,
- spremljanje in beleženje nadzora dostopa do shranjevalnega polja in datotek v skupni rabi oziroma tistih, ki so dostopne preko skupnih programskih vmesnikov API,
- uporaba kriptografske zaščite in šifriranje podatkov, v kolikor je to mogoče, če ne celo zahtevano glede na podatke, ki jih shranjujemo,
- urejena politika izbrisa podatkov s fizičnih shranjevalnih medijev ob odstranitvi oziroma izbrisu navideznega računalnika stanovalca, da preprečimo možnost, da bi novi stanovalec dobil v uporabo shranjevalno polje prejšnjega stanovalca.

3.7 Platforma za upravljanje zasebnega oblaka

Storitev, ki povezuje vse zgoraj naštete komponente in jih združuje v računalništvo v oblaku, je platforma za upravljanje. Predstavlja centralno enoto za celovito upravljanje, nadzor, avtomatizacijo in orkestracijo posameznih komponent in ostalih storitev v oblaku.

Eden od najpomembnejših tehnoloških vidikov varovanja infrastrukture zasebnega oblaka je posledično dostop do njenih upravljavskih (administratorskih) funkcij, saj te navadno omogočajo dostop do občutljivih podatkov in vseh komponent oblaka mimo uporabniških varnostnih kontrol.

3.7.1 Priporočila za izboljšanje varnosti upravljavske platforme

Povzeto po smernicah varovanja OpenStack [45], programske opreme za gradnjo zasebnega oblaka:

- uporaba programske platforme brez znanih ranljivosti,
- sprotno posodabljanje programske platforme in sledenje popravkom s strani proizvajalca,
- uporaba namenskih, ločenih upravljavskih platform za upravljanje oblačne infrastrukture,
- omejen dostop do upravljavskih platform in programskih vmesnikov API; navadno z dodatno izolacijo in omejenim dostopom iz javnih omrežij. Vse upravljavske funkcije naj bodo dosegljive le iz upravljavskih omrežij oziroma za uporabnike preko omrežij VPN, kjer je to potrebno,
- uporaba obstoječih sistemov za upravljanje z identitetami in določanje pravic dostopa do funkcionalnosti,
- močno overjanje upravljavcev in skrbnikov (močna gesla) in izvajanje politike najmanjšega privilegija za dodajanje pravic dostopa do funkcionalnosti,
- uporaba protokola TLS/SSL na vseh komunikacijskih poteh in programskih vmesnikih API,
- beleženje vseh upravljavskih dostopov do infrastrukture in sprotno preverjanje vseh dnevnikov dostopov,
- striktno preverjanje pravic in kontrole dostopa do virov upravljavske platforme,

- v primeru lastnega razvoja določenih upravljavskih komponent upoštevanje priporočil OWASP *(Open Web Application Security Project)* za razvoj varnih spletnih aplikacij in izvajanje varnostnih testiranj razvite programske kode.

3.8 Drugi vidiki varnosti oblačnih storitev

Če smo v vseh prejšnjih poglavjih podajali smernice za čim bolj varno infrastrukturo in okolje, ki poganja zasebni oblak, ne smemo pozabiti na varnost operacijskih sistemov in aplikacij, ki tečejo na tovrstni infrastrukturi, in njihovo varno uporabo. Na tem nivoju velja še vedno upoštevati naslednje[46]:

- uporaba operacijskega sistema, ki je podprt za izbrano virtualizacijsko platformo,
- sprotno posodabljanje operacijskega sistema in sledenje varnostnim popravkom proizvajalca,
- uporaba protivirusne programske opreme in orodij za zaznavanje zlonamerne programske opreme,
- izbira ustreznih gesel in politike gesel, ki uporabnikom narekuje uporabo močnih gesel,
- izklop nepotrebnih servisov in programja,
- uporaba požarne pregrade na nivoju operacijskega sistema in s tem dodatno filtriranje prometa IP,
- uporaba sistemov za preprečevanje ali zaznavanje vdorov (angl. Intrusion Detection/Prevention System) na nivoju operacijskega sistema *(primer: OSSEC, Tripwire)*,
- dostop na daljavo samo preko močnih kriptografskih protokolov za šifriranje komunikacijskih poti in samo za privilegirane uporabnike,

- uporaba pravila najmanjšega privilegija za aplikacije, ki tečejo na sistemu,
- beleženje dostopov, spremljanje konfiguracije in izvajanje varnostne presoje.

Poglavje 4

Zaključek

Računalništvo v oblaku je nedvomno naslednji logični korak v evoluciji virtualizacije obstoječih podatkovnih centrov in nadgradnja klasične infrastrukture IT. Prvi korak je nedvomno izgradnja lastnega zasebnega oblaka. Vsekakor pa si je smiselno za izgradnjo lastnega oblaka vzeti dovolj časa za načrt in odločitev, ali bomo ustrezno platformo kupili, najeli ali vzpostavili na odprtokodni rešitvi. Vsaka od teh odločitev ima določene prednosti in tudi pomanjkljivosti. Pri tem moramo vsekakor upoštevati vsa potencialna varnostna in funkcionalna tveganja, ki so posledica prehoda v oblak ne glede na izbrano tehnologijo ali platformo.

V diplomskem delu smo pregledali največja varnostna tveganja, katerim je računalništvo v oblaku izpostavljeno. Ker je področje računalništva v oblaku obsežno in se še širi, smo se v diplomskem delu osredotočili zgolj na zasebni oblak kot najbolj "varno" obliko postavitvenega modela računalništva v oblaku. Cilj diplomskega dela je bil pripraviti smernice za varen prehod v zasebni oblak. Ko govorimo o varnosti v oblaku, je ključni poudarek na varnosti podatkov in načinih ustreznega zavarovanja osebnih podatkov v skladu s slovensko zakonodajo in posredno tudi z evropskimi direktivami. V ta namen smo pregledali primarna varnostna tveganja posamezne komponente infrastrukture zasebnega oblaka. Na podlagi pregledanih dobrih varnostnih praks, varnostnih standardov in priporočil posameznih proizvajalcev pro-

gramske in strojne opreme za gradnjo storitev računalništva v oblaku smo podali usmeritve tega, s katerimi tehničnimi sredstvi ta tveganja izničimo ali vsaj omilimo.

Še vedno pa ostaja dejstvo, da ne glede na to, ali gradimo lasten varen zasebni oblak ali ga najemamo, ne smemo zanemariti varnosti na nivoju operacijskega sistema in aplikacij, ki tečejo znotraj navideznih računalnikov oblaka.

V procesu priprave diplomskega dela smo zaznali smiselnost izdaje kontrolnega seznama za posamezne komponente infrastrukture zasebnega oblaka, ki bi vseboval ustrezne preslikave na varnostni standard ISO 27001 po vzoru CCM [12] in bi upravljavcem omogočil, da na enostaven in hiter način preverijo, ali izpolnjujejo najbolj osnovna načela dobrih varnostnih praks pri vzpostavitvi, prehodu vanj in uporabi zasebnega oblaka. Vsem obstoječim upravljavcem, ki so že skladni z varnostnim standardom ISO 27001, pa enostavno razširitev opazovane domene, ki pokriva tudi infrastrukturo in storitve zasebnega oblaka.

Nepogrešljivo izhodišče vzpostavitve ali prehoda v kakršno koli obliko storitev računalništva v oblaka pa še naprej ostaja izpolnitev zahtev Zakona o varstvu osebnih podatkov [14], za kar je Informacijski pooblaščenec RS skupaj s CSA Slovenija že izdal smernice in ustrezen kontrolni seznam [15].

Literatura

[1] (2012) "APC Whitepaper WP-118 Virtualization and Cloud Computing: Optimized Power, Cooling, and Management Maximizes Benefits". Dostopno na: http://www.apcmedia.com/salestools/SNIS-7AULCP/SNIS-7AULCP_R4_EN.pdf

[2] P. Mell, T. Grance, "The NIST Definition of Cloud Computing Special Publication 800-145", September 2011. Dostopno na: http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[3] R. Buyya, J. Broberg, A. Goscinski, "Cloud Computing: Principles and Paradigms", Wiley, 2011, pogl. 1

[4] (2013) Spletno mesto "CSA Top threats". Dostopno na: https://cloudsecurityalliance.org/research/top-threats/

[5] (2010) CSA, "Top Threats to Cloud Computing v1.0". Dostopno na: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[6] (2013) CSA, "The Notorious Nine Cloud Computing Top Threats". Dostopno na: https://cloudsecurityalliance.org/download/the-notorious-nine-cloud-computing-top-threats-in-2013/

[7] R. Moen, C. Norman, "Evolution of the PDCA Cycle". Dostopno na: http://pkpinc.com/files/NA01MoenNormanFullpaper.pdf

[8] (2012) Družba Intel, "Planning Guide - Cloud Security". Dostopno na: http://www.intel.com/content/dam/www/public/us/en/documents/guides/cloud-computing-security-planning-guide2.pdf

[9] (2010) Amazon, "Architecting for the Cloud: Best Practices". Dostopno na: http://wwwnew.cs.princeton.edu/courses/archive/spring11/cos448/web/docs/week7_reading2.p

[10] (2013) ENISA, "Certification in the EU Cloud Strategy". Dostopno na: https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy]

[11] (2014) CSA, "STAR Certification Guidance Document: Auditing the Cloud Controls Matrix (CCM)". Dostopno na: https://cloudsecurityalliance.org/research/ocf/#_resources

[12] (2014) CSA, "Cloud Controls Matrix". Dostopno na: https://cloudsecurityalliance.org/research/ccm/

[13] (2014) "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data". Dostopno na: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046

[14] (2007) "Zakon o varstvu osebnih podatkov (uradno prečiščeno besedilo) (ZVOP-1-UPB1)", Uradni List RS, stran 12707, 2007. Dostopno na: http://www.uradni-list.si/1/content?id=82668

[15] (2012) "Varstvo osebnih podatkov in računalništvo v oblaku". Dostopno na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_rac_v_oblaku.pdf

[16] (2004) "Uradni list RS", št. 83/2004 z dne 20.8.2014. Dostopno na: http://www.uradni-list.si/1/objava.jsp?urlid=200483&stevilka=3735

[17] (2011) APC, "Physical Security in Mission Critical Facilities". Dostopno na:
http://www.apcmedia.com/salestools/SADE-5TNRPL/SADE-5TNRPL_R2_EN.pdf

[18] J. Rutkowska, "Subverting Vista Kernel for fun and profit", *konferenca Black Hat Las Vegas*, 2006. Dostopno na:
http://mirror7.meh.or.id/Windows/rootkit/BH-US-06-Rutkowska.pdf

[19] S. T. King, P. M. Chen, "SubVirt: Implementing malware with virtual machines", *IEEE Symposium on Security and Privacy*, 2006

[20] (2009) "Cloudburst". Dostopno na:
https://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-PAPER.pdf

[21] (2011) N. Elhage, "Virtunoid: Breaking out of KVM", *konferenca Defcon 19*, Las Vegas, 2011. Dostopno na:
https://nelhage.com/talks/kvm-defcon-2011.pdf

[22] (2011) "VMware Security Advisories / VMSA-2011-0009.3". Dostopno na:
http://www.vmware.com/security/advisories/VMSA-2011-000

[23] (2013) M. Luft, P. Turbing, "Exploiting Virtual File Formats For Fun and Profit". Dostopno na:
https://www.ernw.de/download/ERNW_Newsletter_41_ExploitingVirtualFileFormats_si

[24] (2014) "Security of the VMware vSphere® Hypervisor". Dostopno na:
https://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

[25] (2009) "Microsoft Hyper-V Security Guide". Dostopno na:
http://www.microsoft.com/en-us/download/details.aspx?id=16650

[26] (2013) "Red Hat Enterprise Linux 6 Virtualization Security Guide Securing your virtual environment". Dostopno na: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Virtualization_Security_Guide/Red_Hat_Enterprise_Linux 6-Virtualization_Security_Guide-en-US.pdf

[27] (2009) Citrix, "Citrix XenServer 5.5.0 User Security". Dostopno na: http://support.citrix.com/servlet/KbServlet/download/20639-102-665890/user_security-1.0-5.5.0-en_gb.pdf

[28] (2012) Positive Tehnologies, "Citrix Xen Server Free/advanced 5.6 Hardening Guide". Dostopno na: http://www.ptsecurity.com/download/XenServer-Free-5-6-SHG.pdf

[29] (2011) NIST, "Guide to Security for Full Virtualization Technologies". Dostopno na: http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf

[30] (2011) W. Jansen, T. Grance, "Guidelines on Securiy and Privacy in Public Cloud Computing". Dostopno na: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494

[31] J. Szefer, E. Keller, R. B. Lee, J. Rexford, "Eliminating the Hypervisor Attack Surface for a More Secure Cloud", *Proceedings of the 18th ACM conference on Computer and communications security*, 2011.

[32] (2011) "PCI DSS Virtualization Guidelines". Dostopno na: https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

[33] (2011) "IEEE Std 802.1Q", *IEEE Computer Society*. Dostopno na: http://standards.ieee.org/getieee802/download/802.1Q-2011.pdf

[34] A. Khan, A. Zugenmaier, D. Jurca, W. Kellerer, "Network virtualization: a hypervisor for the Internet?", *IEEE Communications Magazine*, št. 50, zv. 1, 2012.

[35] K. Hyojoon, N. Feamster, "Improving network management with software defined networking", *IEEE Communication Megazine*, št. 51, zv. 2, 2013.

[36] T. Kiravuo, M. Sarela, J. Manner, "A Survey of Ethernet LAN Security", *IEEE Communications Surveys & Tutorials*, št. 5, zv. 3, 2013.

[37] S. Hansman, R. Hunt, "A taxonomy of network and computer attacks", *Computers & Security*, št. 24, zv. 1, 2005.

[38] (2013) "NIST Cloud Computing Security Reference Architecture". Dostopno na:
http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/CloudSecurity

[39] K. Z. Meth, J. Satran., "Design of the iSCSI protocol", *IEEE Symposium on Mass Storage Systems*, April 2003.

[40] "Amazon S3 Product Details". Dostopno na:
https:aws.amazon.com/s3/details/

[41] "Openstack Swift documentation". Dostopno na:
http:docs.openstack.org/developer/swift/

[42] Ceph domača spletna stran. Dostopna na:
http://ceph.com/

[43] (2010) "Hypervisor Storage Interfaces for Storage Optimization White Paper". Dostopno na:
http://www.snia.org/sites/default/files/HSI_Copy_Offload_WP-r12.pdf

[44] (2012) R. Bouchard, "Securing Fibre Channel Fabrics". Dostopno na:
http://www.brocade.com/downloads/documents/books/SFCF.book_eBook.pdf

[45] OpenStack Foundation, "OpenStack Security Guide". Dostopno na:
http://docs.openstack.org/security-guide/content/index.html

[46] (2008) K. Scarfone, W. Jansen, M. Tracy, "Guide to General Server Security / NIST Special Publication 800-123". Dostopno na: http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf